

Kaspersky Anti-Virus 2010

BENUTZERHANDBUCH

PROGRAMMVERSION: 9.0 CRITICAL FIX 2



KASPERSKY lab

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Achtung! Jedwedes Kopieren, Weiterbreiten oder zum Beispiel Übersetzen von Unterlagen wird nur schriftlich von Kaspersky Lab genehmigt.

Das Dokument und dazu gehörenden Grafiken dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Das Dokument darf ohne vorherige Benachrichtigung geändert werden. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse <http://www.kaspersky.com/de/docs>.

Für den Inhalt, die Güte, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab Ltd. die Haftung ab.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechtsinhaber sind.

Redaktionsdatum: 08.10.2009

© 1997-2009 Kaspersky Lab ZAO

<http://www.kaspersky.de>
<http://support.kaspersky.de>

INHALT

EINLEITUNG	9
Lieferumfang	9
Service für registrierte Benutzer	9
Hard- und Softwarevoraussetzungen für das System	10
KASPERSKY ANTI-VIRUS 2010	11
Suche nach Informationen über das Programm	11
Informationsquellen zur selbständigen Recherche	11
Kontaktaufnahme mit der Vertriebsabteilung	12
Kontaktaufnahme mit dem technischen Support	12
Diskussion über die Programme von Kaspersky Lab im Webforum	13
NEUERUNGEN IN KASPERSKY ANTI-VIRUS 2010	14
SCHUTZKONZEPT FÜR IHREN COMPUTER	15
Schutzkomponenten	15
Aufgaben zur Virensuche	17
Update	17
Schutz für Daten und Online-Aktivität	17
Assistenten und Werkzeuge	18
Servicefunktionen des Programms	18
KASPERSKY ANTI-VIRUS AUF EINEM COMPUTER INSTALLIEREN	20
Schritt 1. Nach neuer Programmversion suchen	21
Schritt 2. Systemkompatibilität für Installation prüfen	21
Schritt 3. Installationstyp auswählen	21
Schritt 4. Lizenzvereinbarung anzeigen	22
Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network	22
Schritt 6. Installationsverzeichnis auswählen	22
Schritt 7. Programmkomponenten für Installation auswählen	23
Schritt 8. Programmeinstellungen einer Vorgängerversion verwenden	23
Schritt 9. Nach anderen Antiviren-Anwendungen suchen	24
Schritt 10. Programminstallation abschließend vorbereiten	24
Schritt 11. Installationsvorgang abschließen	24
ERSTE SCHRITTE	26
Konfigurationsassistent des Programms	26
Schritt 1. Programm aktivieren	27
Kommerzielle Version aktivieren	28
Testversion aktivieren	28
Aktivierung abschließen	28
Schritt 2. Schutzmodus auswählen	28
Schritt 3. Programm-Update anpassen	29
Schritt 4. Kontrolle des Zugriffs auf das Programm	29
Schritt 5. Erkennbare Bedrohungen auswählen	30
Schritt 6. Assistenten abschließen	30
Programm-Update	30
Virenuntersuchung des Computers	31
Untersuchung des Computers auf Schwachstellen	31

Lizenzverwaltung	31
Teilnahme an Kaspersky Security Network	32
Sicherheitsverwaltung.....	33
Schutzstatus	35
Schutz anhalten	35
PROGRAMMOBERFLÄCHE.....	37
Symbol im Infobereich der Taskleiste	37
Kontextmenü.....	38
Hauptfenster von Kaspersky Anti-Virus	39
Meldungen	41
Programmkonfigurationsfenster	41
SCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS.....	42
Algorithmus für die Arbeit der Komponente	43
Sicherheitsstufe für Dateien und Speicher ändern.....	44
Aktion für gefundene Objekte ändern	44
Schutzbereich festlegen.....	45
Heuristische Analyse verwenden	46
Untersuchung optimieren.....	47
Untersuchung von zusammengesetzten Dateien	47
Untersuchung umfangreicher zusammengesetzter Dateien	47
Untersuchungsmodus ändern.....	48
Untersuchungstechnologie	48
Komponente anhalten: Zeitplan erstellen.....	49
Komponente anhalten: Liste der Programme erstellen	50
Standardmäßige Schutzparameter wiederherstellen	51
E-MAIL-SCHUTZ.....	52
Algorithmus für die Arbeit der Komponente	53
Sicherheitsstufe für den E-Mail-Schutz ändern.....	53
Aktion für gefundene Objekte ändern	54
Schutzbereich festlegen.....	55
E-Mail-Untersuchung in Microsoft Office Outlook	55
E-Mail-Untersuchung in The Bat!	56
Heuristische Analyse verwenden	57
Untersuchung von zusammengesetzten Dateien	57
Anlagenfilterung	57
Standardparameter für den Mail-Schutz wiederherstellen	58
SCHUTZ FÜR WEB-DATENVERKEHR.....	59
Algorithmus für die Arbeit der Komponente	60
Sicherheitsstufe für den HTTP-Datenverkehr ändern	61
Aktion für gefundene Objekte ändern	61
Schutzbereich festlegen.....	62
Untersuchungstyp auswählen.....	62
Modul zur Link-Untersuchung	63
Heuristische Analyse verwenden	64
Untersuchung optimieren.....	64
Standardparameter für den Web-Schutz wiederherstellen	65

SCHUTZ FÜR DEN DATENVERKEHR VON INSTANT-MESSENGERN	66
Algorithmus für die Arbeit der Komponente	67
Schutzbereich festlegen.....	67
Untersuchungsmethode auswählen.....	67
Heuristische Analyse verwenden	68
PROAKTIVER SCHUTZ.....	69
Liste der gefährlichen Aktivität verwenden.....	69
Kontrollregel für gefährliche Aktivität ändern	70
Gruppe mit vertrauenswürdigen Programmen erstellen.....	71
Kontrolle über Systembenutzerkonten	71
UNTERSUCHUNG DES COMPUTERS	72
Virensuche.....	72
Start der Untersuchungsaufgabe	74
Verknüpfung für den Aufgabenstart erstellen	75
Liste der Untersuchungsobjekte erstellen	75
Sicherheitsstufe ändern.....	76
Aktion beim Fund einer Bedrohung ändern.....	76
Typ der zu untersuchenden Objekte ändern	77
Untersuchung optimieren	78
Wechseldatenträger untersuchen	78
Untersuchung von zusammengesetzten Dateien.....	79
Untersuchungstechnologie.....	79
Untersuchungsmethode ändern	80
Startmodus: Zeitplan erstellen.....	81
Startmodus: Benutzerkonto festlegen	81
Besonderheiten beim Start von geplanten Untersuchungsaufgaben	82
Standardmäßige Untersuchungseinstellungen wiederherstellen.....	82
Suche nach Schwachstellen	82
Aufgabe zur Suche nach Schwachstellen starten	83
Verknüpfung für den Aufgabenstart erstellen.....	84
Liste der Untersuchungsobjekte erstellen	84
Startmodus: Zeitplan erstellen.....	85
Startmodus: Benutzerkonto festlegen	85
UPDATE.....	87
Update starten	88
Rollback zum vorherigen Update	89
Updatequelle auswählen.....	89
Proxyserver verwenden	90
Regionsoptionen.....	90
Aktionen nach dem Update.....	90
Update aus einem lokalen Ordner	91
Startmodus für die Updateaufgabe ändern.....	91
Updatestart mit den Rechten eines anderen Benutzers.....	92
PROGRAMMPARAMETER ANPASSEN	93
Schutz.....	94
Computerschutz aktivieren / deaktivieren.....	94
Kaspersky Anti-Virus beim Hochfahren des Betriebssystems starten	95

Interaktiven Schutzmodus verwenden	95
Kontrolle des Zugriffs auf Kaspersky Anti-Virus	96
Datei-Anti-Virus.....	96
Mail-Anti-Virus	97
Web-Anti-Virus.....	98
IM-Anti-Virus	99
Proaktiver Schutz.....	99
Untersuchung	100
Update	101
Einstellungen	101
Selbstschutz für Kaspersky Anti-Virus.....	101
Technologie zur Desinfektion einer aktiven Infektion	102
Arbeit von Kaspersky Anti-Virus auf einem Laptop	102
Leistung des Computers beim Ausführen von Aufgaben	103
Funktionsparameter für Kaspersky Anti-Virus exportieren / importieren	103
Standardparameter wiederherstellen	104
Bedrohungen und Ausnahmen.....	104
Kategorien der erkennbaren Bedrohungen auswählen	105
Vertrauenswürdige Programme auswählen.....	105
Regeln für Ausnahmen.....	106
Netzwerk	108
Liste der zu kontrollierenden Ports erstellen.....	108
Untersuchung geschützter Verbindungen	109
Untersuchung geschützter Verbindungen in Mozilla Firefox.....	110
Untersuchung geschützter Verbindungen in Opera.....	111
Proxyserver-Einstellungen.....	112
Meldungen	112
Audiosignale zur Begleitung von Benachrichtigungen deaktivieren.....	113
E-Mail-Benachrichtigungen senden.....	113
Berichte und Speicher.....	113
Einträge über Ereignisse zum Bericht hinzufügen	114
Berichte leeren	114
Berichte speichern.....	114
Quarantäne für möglicherweise infizierte Objekte	115
Sicherungskopien gefährlicher Objekte	116
Arbeit mit Objekten in der Quarantäne	116
Quarantäne- und Backup-Objekte speichern	116
Feedback	117
Aussehen des Programms	117
Aktive Elemente der Benutzeroberfläche	117
Grafische Oberfläche von Kaspersky Anti-Virus.....	118
Profile für Kaspersky Anti-Virus verwenden	118
ZUSÄTZLICHE OPTIONEN	120
Virtuelle Tastatur.....	120
Notfall-CD	121
Notfall-CD erstellen	122
Hochfahren eines Computers mit Hilfe der Notfall-CD	122
Browser-Konfiguration	123

Wiederherstellung nach Infektion.....	124
Assistent zum Löschen von Aktivitätsspuren	125
BERICHTE	126
Komponente oder Aufgabe für das Erstellen eines Berichts auswählen.....	126
Anordnung von Informationen im Bericht.....	127
Über Bereitschaft des Berichts benachrichtigen	127
Ereignistyp auswählen	128
Darstellung von Daten auf dem Bildschirm	129
Erweiterte Statistikanzeige.....	130
Bericht in Datei speichern	130
Verwendung der komplexen Filterung	130
Suche nach Ereignissen	131
MELDUNGEN	133
Verdächtiges Objekt wurde gefunden	134
Desinfektion des Objekts ist nicht möglich.....	135
Spezielle Desinfektionsprozedur ist erforderlich	135
Gefährliches Objekt wurde im Datenstrom gefunden	136
Verdächtiges Objekt wurde gefunden.....	136
Gefährliche Aktivität im System wurde erkannt.....	137
Versteckter Prozess wurde gefunden	138
Versuch zum Zugriff auf die Systemregistrierung wurde erkannt.....	138
Phishing-Angriff wurde erkannt.....	139
Verdächtiger Link wurde gefunden	139
Ein inkorrektes Zertifikat wurde gefunden.....	139
EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS AUF KORREKTHEIT PRÜFEN.....	141
EICAR-"Testvirus" und seine Modifikationen	141
Testen des Schutzes für HTTP-Datenverkehr	143
Schutz für den SMTP-Datenverkehr testen	143
Überprüfung der Einstellungen von Datei-Anti-Virus	143
Überprüfung der Einstellungen für eine Aufgabe zur Virensuche	144
BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE.....	145
Steuerung von Komponenten und Aufgaben des Programms.....	146
Virensuche.....	148
Programm-Update	151
Rollback zum vorherigen Update	151
Schutzparameter exportieren.....	152
Schutzparameter importieren.....	152
Programm starten	153
Programm beenden	153
Protokolldatei anlegen	153
Hilfe anzeigen	154
Rückgabecodes der Befehlszeile.....	154
PROBLEME BEHEBEN	155
Bericht über den Systemzustand erstellen.....	155
Protokolldatei erstellen.....	156
Dateien mit Daten senden	156
AVZ-Skript ausführen.....	157

ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK	159
VERWENDUNG DES CODES VON DRITTHERSTELLERN	160
Bibliothek (PBSI) "Crypto-Si"	161
Bibliothek fastscript 1.9	162
Bibliothek pcre 7.4, 7.7	162
Bibliothek GNU bison parser	162
Bibliothek AGG 2.4	163
Bibliothek OpenSSL 0.9.8d	163
Bibliothek Gecko SDK 1.8	165
Bibliothek zlib 1.2	165
Bibliothek libpng 1.2.08, 1.2.29	165
Bibliothek libnfm 2.0.5	165
Bibliothek expat 1.2, 2.0.1	165
Bibliothek Info-ZIP 5.51	166
Bibliothek Windows Installer XML (WiX) 2.0	166
Bibliothek passthru	169
Bibliothek filter	169
Bibliothek netcfg	169
Bibliothek pcre 3.0	169
Bibliothek RFC1321-based (RSA-free) MD5 library	169
Bibliothek Windows Template Library (WTL 7.5)	170
Bibliothek libjpeg 6b	172
Bibliothek libungif 3.0	174
Bibliothek libxdr	174
Bibliothek tiniconv - 1.0.0	174
Bibliothek bzip2/libbzip2 1.0.5	179
Bibliothek libspf2-1.2.9	180
Bibliothek Protocol Buffer	180
GLOSSAR	182
ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE	191
KASPERSKY LAB	197
KASPERSKY LAB	198
SACHREGISTER	199

EINLEITUNG

IN DIESEM ABSCHNITT

Lieferumfang	9
Service für registrierte Benutzer	9
Hard- und Softwarevoraussetzungen für das System	10

LIEFERUMFANG

Sie können Kaspersky Anti-Virus bei unseren Fachhändlern (als Box mit CD) sowie im Online-Shop kaufen <http://www.kaspersky.de>.

Haben Sie das Programm in einer Box erworben, gehören zum Lieferumfang des Programms:

- Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Gedrucktes Benutzerhandbuch und eine Quick-Start-Anleitung (nicht bei allen Box-Typen enthalten).
- Lizenzvereinbarung.
- Aktivierungskarte mit Aktivierungscode und Anleitung zur Aktivierung des Programms.

Die Lizenzvereinbarung ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab, in dem steht, unter welchen Bedingungen Sie das von Ihnen gekaufte Programm gebrauchen dürfen.

Lesen Sie sich die Lizenzvereinbarung genau durch!

Wenn Sie die Bedingungen der Lizenzvereinbarung nicht annehmen, können Sie die Box an den Fachhändler zurückgeben, bei dem Sie sie gekauft haben, und Sie bekommen Ihr Geld zurück.

Bevor Sie das Programm installieren, lesen Sie sich bitte die Lizenzvereinbarung sorgfältig durch.

Beim Kauf von Kaspersky Anti-Virus im Online-Shop kopieren Sie das Programm sowie dieses Handbuch von der Webseite von Kaspersky Lab. Der Aktivierungscode wird Ihnen per E-Mail nach Eingang des Rechnungsbetrages zugestellt.

SERVICE FÜR REGISTRIERTE BENUTZER

Wenn Sie eine Lizenz erwerben, werden Sie ein registrierter Benutzer und während der Gültigkeitsdauer der Lizenz können Sie folgende Leistungen in Anspruch nehmen:

- Stündliche Updates der Programm-Datenbanken und kostenlose Upgrades neuer Programmversionen.
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail.
- Benachrichtigung über neue Versionen und neu aufgetauchte Viren. Dieser Service wird Benutzern geboten, die den Newsletter von Kaspersky Lab auf der Webseite des technischen Supports (<http://support.kaspersky.com/de/subscribe/>) abonniert haben.

Der technische Support kann leider keine Fragen zu Funktion und Gebrauch von Betriebssystemen, zu Programmen von Dritten sowie zu verschiedenen Technologien beantworten.

HARD- UND SOFTWAREVORAUSSETZUNGEN FÜR DAS SYSTEM

Um die normale Funktionsfähigkeit von Kaspersky Anti-Virus 2010 zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Allgemeine Anforderungen:

- 375 MB freier Speicherplatz auf der Festplatte.
- CD-ROM-Laufwerk (für die Installation von Kaspersky Anti-Virus 2010 von Installations-CD).
- Microsoft Internet Explorer 6.0 oder höher (für Updates der Datenbanken und Programm-Module über das Internet).
- Microsoft Windows Installer 2.0.
- *Microsoft Windows XP Home Edition (Service Pack 2), Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition:*
 - Intel Pentium 300 MHz oder höher (oder kompatibel).
 - 256 MB Arbeitsspeicher.
- *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*
 - Prozessor Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
 - 512 MB Arbeitsspeicher.
- *Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*
 - Prozessor Intel Pentium 1 MHz 32-bit (x86)/ 64-bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
 - 1 GB Arbeitsspeicher (32-bit); 2 GB Arbeitsspeicher (64-bit).

KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 ist eine neue Generation von Schutzprogrammen.

Der Hauptunterschied zwischen Kaspersky Anti-Virus 2010 und den restlichen Produkten von Kaspersky Lab, besteht in den komplexen Methoden zum Schutz der Daten auf einem Computer.

IN DIESEM ABSCHNITT

Suche nach Informationen über das Programm [11](#)

SUCHE NACH INFORMATIONEN ÜBER DAS PROGRAMM

Wenn Sie Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Anti-Virus haben, können Sie schnell eine Antwort darauf erhalten.

Kaspersky Lab bietet unterschiedliche Informationsquellen zu dem Programm an. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage unter diesen Quellen wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche [11](#)

Kontaktaufnahme mit der Vertriebsabteilung [12](#)

Kontaktaufnahme mit dem technischen Support [12](#)

Diskussion über die Programme von Kaspersky Lab im Webforum [13](#)

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

Seite auf der Webseite von Kaspersky Lab

http://www.kaspersky.de/kaspersky_anti-virus

Auf dieser Seite finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Webseite des technischen Supports (Wissensdatenbank)

<http://support.kaspersky.de/kav2010>

Auf dieser Seite finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung der Programme von Kaspersky Lab. Die Artikel können auch Fragen behandeln, die neben diesem Programm auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie allgemeine Neuigkeiten über den technischen Support enthalten.

Interaktiver Support

Auf der Seite dieses Dienstes finden Sie eine regelmäßig aktualisierte Datenbank von häufig gestellten Fragen und Antworten. Um diesen Dienst nutzen zu können, ist eine Internetverbindung erforderlich.

Um zur Seite für diesen Dienst zu wechseln, klicken Sie im Programmhauptfenster auf den Link **Support** und im folgenden Fenster auf die Schaltfläche **Interaktiver Support**.

Elektronisches Hilfesystem

Im Lieferumfang des Programms ist eine vollständige und kontextorientierte Hilfedatei enthalten. Sie bietet Informationen zu folgenden Aspekten der Verwaltung des Computerschutzes: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben, sowie Informationen zu jedem Fenster der Anwendung: Liste und Beschreibung der in einem Fenster vorhandenen Parameter und Liste der ausführbaren Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im entsprechenden Fenster auf die Schaltfläche **Hilfe** oder auf die Taste **<F1>**.

Dokumentation

Zum Lieferumfang von Kaspersky Anti-Virus gehört das Dokument **Benutzerhandbuch** (im PDF-Format). Es enthält eine ausführliche Beschreibung aller Funktionen.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von Kaspersky Anti-Virus sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in unserer Zentrale in Moskau unter folgenden Telefonnummern zur Verfügung:

+49 (0)841 – 981 89 560

Sie können sich mit Ihrer Frage auch unter folgender Adresse per E-Mail an die Mitarbeiter der Vertriebsabteilung wenden: vertrieb@kaspersky.de.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie die Kaspersky Anti-Virus bereits erworben haben, können Sie von den Spezialisten des Technischen Supports per Telefon oder über das Internet Informationen darüber erhalten.

Die Spezialisten des technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Bevor Sie sich an den technischen Support wenden, lesen Sie sich bitte zuvor Supportrichtlinien (<http://support.kaspersky.com/de/support/rules>) durch.

E-Mail-Anfrage an den technischen Support

Die Support-Spezialisten werden Ihre Frage in Ihrem Personal Cabinet (<https://my.kaspersky.com/de>) und per E-Mail an die in der Anfrage angegebene Adresse beantworten.

Beschreiben Sie im Webformular das aufgetretene Problem möglichst genau. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Typ der Anfrage.** Wählen Sie die Problemart aus, dem Ihr Problem möglichst nahe kommt.
- **Name und Versionsnummer des Programms.**
- **Anfragetext.** Beschreiben Sie das Problem möglichst genau.
- **E-Mail-Adresse.** An diese Adresse werden die Support-Spezialisten Ihre Anfrage beantworten.

Technischer Support am Telefon

Zur Lösung dringender Probleme können Sie den lokalen technischen Support anrufen. Informationen hierzu finden Sie unter www.kaspersky.de/technischer_support.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse <http://forum.kaspersky.com> diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

NEUERUNGEN IN KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 ist ein universelles Programm für den Informationsschutz. Der komplexe Schutz wird auf allen Kanälen gewährleistet, auf denen Daten eingehen und übertragen werden. Flexible Einstellungsmöglichkeiten für alle Komponenten erlauben es, Kaspersky Anti-Virus präzise an die Erfordernisse eines konkreten Benutzers anzupassen.

Ausführliche Beschreibung der Neuerungen in Kaspersky Anti-Virus 2010

Neuerungen im Schutz:

- Die neue Komponente IM-Anti-Virus (s. S. [66](#)) gewährleistet Sicherheit bei der Arbeit mit den meisten Programmen zum schnellen Nachrichtenaustausch. Die Komponente untersucht Nachrichten auf das Vorhandensein gefährlicher Objekte.
- Kaspersky Anti-Virus umfasst ein Modul zur Link-Untersuchung (s. S. [63](#)), das zu der Komponente Web-Anti-Virus gehört. Das Modul untersucht alle Links, die auf einer Webseite vorhanden sind, auf Zugehörigkeit zu verdächtigen und Phishing-Webadressen. Das Modul wird als Plug-in in die Webbrowser Microsoft Internet Explorer und Mozilla Firefox integriert.
- Der Zugriff auf Phishing-Webadressen und der Schutz vor Phishing-Angriffen werden durch die Untersuchung von Links kontrolliert, die in Nachrichten und auf Webseiten enthalten sind. Außerdem werden Zugriffsversuche auf Webseiten mit einer Datenbank für Phishing-Webadressen überwacht. Die Untersuchung der Zugehörigkeit zu der Datenbank für Phishing-Webadressen ist für Web-Anti-Virus (s. S. [62](#)) und IM-Anti-Virus (s. S. [67](#)) verfügbar.
- Die Liste der Untersuchungsaufgaben wurde um das neue Tool Suche nach Schwachstellen (s. S. [82](#)) erweitert. Es erleichtert die Suche und Neutralisierung von Sicherheitsrisiken und Schwachstellen in den auf Ihrem Computer installierten Programmen und in den Parametern des Betriebssystems.

Neuerungen auf der Programmoberfläche:

- Mit dem Schutz-Center wurde eine neue Methode zur Verwaltung des Schutzes realisiert. Dateien und persönliche Benutzerdaten, Objekte des Betriebssystems und auf dem Computer installierte Programme unter Kontrolle, ebenso die Arbeit im Netzwerk. Für jeden Aspekt des Schutzes ist eine spezielle Auswahl der Komponenten von Kaspersky Anti-Virus verantwortlich. Unter Verwendung des Schutz-Centers kann der Benutzer beurteilen, welche Komponente am Schutz einer bestimmten Ressourcenkategorie beteiligt ist, und schnell zu den entsprechenden Einstellungen gelangen.
- Assistenten und Werkzeuge (s. S. [18](#)), mit denen spezifische Aufgaben im Bezug auf die Computersicherheit gelöst werden können, sind im Abschnitt **Sicherheit+** zusammengefasst.

SCHUTZKONZEPT FÜR IHREN COMPUTER

Kaspersky Anti-Virus schützt Ihren Computer vor bekannten und neuen Bedrohungen. Jeder Bedrohungstyp wird von einer bestimmten Programmkomponente verarbeitet. Dieser Aufbau des Schutzsystems erlaubt es, das Programm flexibel an die Erfordernisse eines konkreten Benutzers oder Unternehmens anzupassen.

Kaspersky Anti-Virus verfügt über folgende Schutzwerkzeuge:

- Schutzkomponenten (s. S. [15](#)), die die Sicherheit gewährleisten:
 - für Dateien und persönliche Daten.
 - für das System.
 - für die Arbeit in einem Netzwerk.
- Aufgaben zur Virensuche (s. S. [17](#)), mit denen die Virensuche in einzelnen Dateien, Ordnern, Laufwerken oder Bereichen, oder die vollständige Untersuchung des Computers erfolgt.
- Update (s. S. [17](#)), das den aktuellen Zustand der internen Programm-Module sowie der Datenbanken, die für die Suche nach schädlichen Programmen verwendet werden, aufrechterhält
- Assistenten und Werkzeuge (s. S. [18](#)), die Aufgaben vereinfachen, die im Verlauf von Kaspersky Anti-Virus auftreten.
- Servicefunktionen (s. S. [18](#)), die Informationen über die Arbeit mit den Programmen bieten und es erlauben, die Programmfunktionalität zu erweitern.

IN DIESEM ABSCHNITT

Schutzkomponenten.....	15
Aufgaben zur Virensuche	17
Update.....	17
Schutz für Daten und Online-Aktivität.....	17
Assistenten und Werkzeuge	18
Servicefunktionen des Programms.....	18

SCHUTZKOMPONENTEN

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Datei-Anti-Virus (s. S. [42](#))

Datei-Anti-Virus kontrolliert das Dateisystem des Computers. Er untersucht auf Ihrem Computer und auf allen angeschlossenen Laufwerken alle Dateien, die geöffnet, gestartet und gespeichert werden. Jeder Zugriff auf eine Datei wird von Kaspersky Anti-Virus abgefangen und die Datei wird auf die Existenz bekannter Viren untersucht. Eine Datei wird nur dann zur Arbeit freigegeben, wenn die Datei virenfrei ist oder erfolgreich vom Programm desinfiziert wurde. Wenn die Desinfektion einer Datei aus irgendwelchen Gründen nicht möglich ist, wird sie gelöscht. Dabei wird ihre Kopie im Backup abgelegt oder in der Quarantäne gespeichert.

Mail-Anti-Virus (s. S. [52](#))

Mail-Anti-Virus untersucht alle ein- und ausgehenden E-Mails auf Ihrem Computer. Er analysiert E-Mails auf die Existenz von Schadprogrammen. Eine E-Mail wird nur dann dem Empfänger zugestellt, wenn sie keine gefährlichen Objekte enthält. Außerdem analysiert die Komponente E-Mails im Hinblick auf Phishing

Web-Anti-Virus (s. S. [59](#))

Web-Anti-Virus fängt die Ausführung von Skripts, die sich auf Webseiten befinden, ab und blockiert sie, falls Sie gefährlich sind. Auch der HTTP-Verkehr unterliegt einer strengen Kontrolle. Außerdem analysiert die Komponente Webseiten im Hinblick auf Phishing.

IM-Anti-Virus (s. S. [66](#))

IM-Anti-Virus sorgt für die Sicherheit bei Instant-Messengern. Sie schützt die Informationen, die über Instant-Messenger-Protokolle auf Ihren Computer gelangen. IM-Anti-Virus gewährleistet Sicherheit bei der Arbeit mit vielen Programmen zum schnellen Nachrichtenaustausch.

Proaktiver Schutz (s. S. [69](#))

Der Proaktive Schutz erlaubt es, ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann. Die Komponente basiert auf der Kontrolle und Analyse des Verhaltens aller auf Ihrem Computer installierten Programme. Aufgrund der auszuführenden Aktionen entscheidet Kaspersky Anti-Virus, ob ein Programm potentiell gefährlich ist oder nicht. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannten Viren geschützt.

Anti-Phishing

Komponente, die in Web-Anti-Virus und IM-Anti-Virus integriert ist und mit der Webadressen auf ihre Zugehörigkeit zur Liste der Phishing- und verdächtigen Webadressen untersucht werden können.

Einige Schutzkomponenten sind nur in Kaspersky Internet Security 2010 verfügbar. Dazu gehören die folgenden Komponenten:

Programmkontrolle

Die Programmkontrolle registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der ein Programm gehört, seine Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen.

Firewall

Die Firewall gewährleistet Sicherheit in lokalen Netzwerken und im Internet. Sie filtert die gesamte Netzwerkaktivität, wozu zwei Arten von Regeln dienen: *Regeln für Programme* und *Paketregeln*.

Schutz vor Netzwerkangriffen

Der Schutz vor Netzwerkangriffen wird beim Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky Anti-Virus jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihren Computer.

Anti-Spam

Anti-Spam wird in Ihr Mailprogramm integriert und kontrolliert alle eingehenden E-Mail auf Spam. Alle E-Mails, die Spam enthalten, werden durch eine spezielle Kopfzeile markiert. Anti-Spam kann zusätzlich für die Spam-Verarbeitung (automatisches Löschen, Verschieben in einen speziellen Ordner, u.a.) eingestellt werden. Außerdem analysiert die Komponente E-Mails im Hinblick auf Phishing

Netzwerkmonitor

Diese Komponente dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Anti-Banner

Anti-Banner blockiert Werbung, die auf speziellen Bannern platziert ist, die in das Interface von auf Ihrem Computer installierten Programmen integriert sind oder sich im Internet befinden.

Kindersicherung

Die Programmkomponente Kindersicherung kontrolliert den Zugriff von Computerbenutzern auf Webressourcen. Die Hauptaufgabe der Kindersicherung besteht darin, den Zugriff auf folgende Ressourcen zu beschränken: Webseiten, die für Erwachsene bestimmt sind oder die Themen wie Pornografie, Waffen, Drogen betreffen oder Grausamkeit, Gewalt usw. provozieren, sowie Webseiten, die Zeitverlust (Chats, Glücksspiel) oder Geldverlust (Online-Shops, Auktionen) verursachen können.

AUFGABEN ZUR VIRENSUCHE

Neben dem Schutz des Computers, ist es sehr wichtig, regelmäßig eine vollständige Virenuntersuchung Ihres Computers durchzuführen. Das ist erforderlich, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Kaspersky Anti-Virus verfügt über folgende Aufgaben zur Virensuche:

- **Objekte untersuchen.** Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.
- **Vollständige Untersuchung.** Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Schnelle Untersuchung.** Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

UPDATE

Um stets bereit zu sein, Netzwerkangriffe abzuwehren und Viren oder andere gefährliche Programme zu neutralisieren, ist es unerlässlich, Kaspersky Anti-Virus immer auf dem neusten Stand zu halten. Dazu dient die Komponente **Update**. Sie ist für die Aktualisierung der Datenbanken und Programm-Module verantwortlich, die bei der Arbeit des Programms verwendet werden.

Der Dienst zur Update-Verteilung erlaubt es, die Updates für Datenbanken und Programm-Module, die von den Kaspersky-Lab-Updateservern heruntergeladen wurden, in einem lokalen Ordner zu speichern. Dieser Ordner kann anderen Netzwerkcomputern als Updatequelle dienen, um Datenverkehr einzusparen.

SCHUTZ FÜR DATEN UND ONLINE-AKTIVITÄT

Kaspersky Anti-Virus schützt die Daten auf Ihrem Computer vor Malware und nicht autorisiertem Zugriff. Außerdem gewährleistet das Programm den sicheren Zugriff auf das lokale Netzwerk und auf das Internet.

Die geschützten Objekte lassen sich in drei Gruppen unterteilen:

- Dateien, persönliche Daten, Einstellungen für den Zugriff auf unterschiedliche Ressourcen (Benutzernamen und Kennwörter), Daten über Scheckkarten usw. Am Schutz dieser Objekte sind Datei-Anti-Virus und Proaktiver Schutz beteiligt.
- Auf Ihrem Computer installierte Programme und Objekte des Betriebssystems. Am Schutz dieser Objekte sind Mail-Anti-Virus, IM-Anti-Virus und Proaktiver Schutz beteiligt.

- Arbeit im Netzwerk: Anzeigen von Seiten, Verwendung von Zahlungssystemen, Schutz des Posteingangs vor Spam und Viren usw. Am Schutz dieser Objekte sind Mail-Anti-Virus, Web-Anti-Virus, IM-Anti-Virus und Anti-Phishing beteiligt.

ASSISTENTEN UND WERKZEUGE

Es ist eine schwierige Aufgabe, die Sicherheit eines Computers zu gewährleisten. Dafür sind Kenntnisse über Besonderheiten der Funktion eines Betriebssystems und über potentielle Schwachstellen erforderlich. Zudem erschweren die große Menge und die Vielfalt der Informationen über die Systemsicherheit deren Analyse und Verarbeitung.

Um spezifische Aufgaben, die die Sicherheit des Computers gewährleisten, zu vereinfachen, verfügt Kaspersky Anti-Virus über unterschiedliche Assistenten und Werkzeuge.

- Der Assistent zur Browser-Konfiguration (s. S. [123](#)) führt eine Analyse der Einstellungen des Browsers Microsoft Internet Explorer aus. Dabei werden die Einstellungen hauptsächlich im Hinblick auf die Sicherheit bewertet.
- Der Assistent zur Wiederherstellung nach einer Infektion (s. S. [124](#)) beseitigt im System die Spuren von schädlichen Objekten.
- Assistent zum Löschen von Aktivitätsspuren (s. S. [125](#)), der nach Aktivitätsspuren des Benutzers im System und Einstellungen des Betriebssystems sucht und beseitigt, die Daten über die Aktivität des Benutzers sammeln.
- Die Notfall-CD (s. S. [121](#)) dient zur Untersuchung und Desinfektion infizierter x86-kompatibler Computer. Sie kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools möglich ist.
- Suche nach Schwachstellen (s. S. [82](#)) diagnostiziert die Sicherheit des Computers und sucht nach Schwachstellen im Betriebssystem und in Programmen, die auf dem Computer installiert sind.
- Virtuelle Tastatur (s. S. [120](#)), sodass keine über die Tastatur eingegebenen Daten erfasst werden können.

SERVICEFUNKTIONEN DES PROGRAMMS

Kaspersky Anti-Virus verfügt über folgende Servicefunktionen: Sie dienen dazu, den aktuellen Zustand des Programms aufrechtzuerhalten, die Optionen des Programms zu erweitern und bei der Arbeit Hilfe zu leisten.

Datenverwaltung und Berichte

Im Programmverlauf wird für jede Schutzkomponente, jede Untersuchungs- oder Updateaufgabe des Programms ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und die Arbeitsergebnisse. Dadurch können Sie jederzeit Details über die Arbeit einer beliebigen Komponente von Kaspersky Anti-Virus nachlesen. Sollten Probleme auftreten, dann können Sie die Berichte an Kaspersky Lab schicken, damit unsere Experten die Situation analysieren und Ihnen möglichst schnell helfen können.

Alle im Hinblick auf die Sicherheit verdächtigen Objekte werden von Kaspersky Anti-Virus in den speziellen Speicher *Quarantäne* verschoben. Sie werden dort in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können die Quarantäneobjekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen oder löschen. Außerdem können Sie verdächtige Objekte manuell in die Quarantäne verschieben. Alle Objekte, die sich aufgrund der Untersuchung als virenfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien von Objekten gespeichert, die von Kaspersky Anti-Virus desinfiziert und gelöscht wurden. Diese Kopien werden angelegt, um bei Bedarf die Objekte oder ein Bild der Infektion wiederherzustellen. Auch die Sicherungskopien der Objekte werden in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen.

Sie können ein Objekt aus dem Backup am ursprünglichen Ort wiederherstellen oder die Sicherungskopie löschen.

Lizenz

Beim Kauf von Kaspersky Anti-Virus wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, auf dessen Grundlage Sie die Anwendung verwenden dürfen und für einen festgelegten Zeitraum Zugriff auf Updates für die Programm-Datenbanken und auf den Technischen Support erhalten. Die Nutzungsdauer sowie andere Informationen, die für die vollfunktionale Arbeit der Anwendung erforderlich sind, sind in der Lizenz angegeben.

Mit der Funktion **Lizenz** können Sie ausführliche Informationen über die von Ihnen verwendete Lizenz erhalten. Außerdem können Sie damit eine neue Lizenz erwerben oder die Gültigkeit der aktiven Lizenz verlängern.

Support

Alle registrierten Benutzer von Kaspersky Anti-Virus können den Technischen Support-Service in Anspruch nehmen. Um die Bedingungen für die Inanspruchnahme zu erfahren, nutzen Sie die Funktion **Support**.

Mit Hilfe der entsprechenden Links gelangen Sie zum Benutzerforum für die Kaspersky-Lab-Produkte oder können auf der Support-Webseite ein Formular mit einer Fehlermeldung oder Rückmeldung über die Arbeit des Programms senden.

Außerdem stehen Ihnen der Technische Support online zur Verfügung, ebenso die Services des Kaspersky Account für einen Benutzer und natürliche persönliche Beratung am Telefon durch unsere Fachleute, die Ihnen immer gern beim Umgang mit Kaspersky Anti-Virus helfen.

KASPERSKY ANTI-VIRUS AUF EINEM COMPUTER INSTALLIEREN

Kaspersky Anti-Virus wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Vor der Installation sollten Sie alle laufenden Programme schließen.

Um Kaspersky Anti-Virus auf Ihrem Computer zu installieren, starten Sie auf der CD-ROM mit dem Programm die ausführbare Datei (mit der Endung *.exe).

Der Installationsvorgang für das Programm Kaspersky Anti-Virus, das aus dem Internet bezogen wurde, ist komplett identisch mit der Installation von der CD-ROM.

Im Anschluss wird nach dem Installationspaket für Kaspersky Anti-Virus gesucht (Datei mit Endung *.msi) und wenn es vorliegt, wird nach einer neuen Version auf den Kaspersky-Lab-Servern im Internet gesucht. Wenn die Datei des Installationspaketes nicht gefunden wird, wird Ihnen der Download vorgeschlagen. Nach dem Download wird die Installation von Kaspersky Anti-Virus gestartet. Sollten Sie den Download nicht wünschen, geht die Installation des Programms normal weiter.

Der Installer ist wie ein Assistent. In jedem Fenster stehen verschiedene Schaltflächen, um den Installationsvorgang zu verwalten. Es folgt eine kurze Beschreibung:

- **Weiter** – Vorgang wird angenommen und es geht weiter zum nächsten Schritt im Installationsvorgang.
- **Zurück** – Rückkehr zum vorangegangenen Schritt der Installation.
- **Abbrechen** – Installation wird abgebrochen.
- **Fertig** – Installationsvorgang des Programms auf dem Computer wird beendet.

Es folgt eine detaillierte Beschreibung jedes Schrittes im Installationsvorgang.

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen	21
Schritt 2. Systemkompatibilität für Installation prüfen	21
Schritt 3. Installationstyp auswählen	21
Schritt 4. Lizenzvereinbarung anzeigen.....	22
Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network.....	22
Schritt 6. Installationsverzeichnis auswählen	22
Schritt 7. Programmkomponenten für Installation auswählen.....	23
Schritt 8. Programmeinstellungen einer Vorgängerversion verwenden	23
Schritt 9. Nach anderen Antiviren-Anwendungen suchen	24
Schritt 10. Programminstallation abschließend vorbereiten.....	24
Schritt 11. Installationsvorgang abschließen	24

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky Anti-Virus auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky Anti-Virus vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Vor der Installation von Kaspersky Anti-Virus auf Ihrem Computer wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation abgeglichen. Außerdem werden die Hardwarevoraussetzungen geprüft sowie die Rechte für die Installation des Programms.

Wenn eine Bedingung nicht eingehalten wird, erscheint auf dem Bildschirm eine entsprechende Meldung. In solchen Fällen sollten vor der Installation des Kaspersky-Lab-Programms die benötigten Service Packs durch Windows Update sowie die nötigen Programme installiert werden.

SCHRITT 3. INSTALLATIONSTYP AUSWÄHLEN

Wenn Ihr System komplett die genannten Voraussetzungen erfüllt, keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde oder Sie die Installation einer neueren Version abgelehnt haben, startet auf Ihrem Computer der Installationsassistent der laufenden Version von Kaspersky anti-Virus.

In dieser Phase der Installation können Sie einen passenden Typ für die Installation von Kaspersky Anti-Virus auswählen:

- *Schnelle Installation.* Bei dieser Variante (das Kontrollkästchen ☐ **Benutzerdefinierte Installation** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert. Nach der Installation wird der Konfigurationsassistent des Programms (auf S. [26](#)) gestartet.
- *Benutzerdefinierte Installation.* In diesem Fall (das Kontrollkästchen ☒ **Benutzerdefinierte Installation** ist aktiviert) können Sie auswählen, welche Programmkomponenten installiert werden sollen und welcher Installationsordner verwendet werden soll. Außerdem können Sie das Programm aktivieren und einen speziellen Assistenten für die Konfiguration verwenden.

Bei der ersten Variante schlägt der Installationsassistent Ihnen vor, zunächst die Lizenzvereinbarung zu lesen und den Gebrauch des Kaspersky Security Network kennen zu lernen. Danach wird das Programm auf Ihrem Computer installiert.

Bei der zweiten Variante müssen Sie in jeder Phase der Installation einige Daten eingeben oder bestätigen.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**. Die Installation lässt sich mit der Schaltfläche **Abbrechen** ablehnen.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkt einverstanden sind, klicken Sie auf die Schaltfläche **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Zum Ablehnen klicken Sie auf die Schaltfläche **Abbrechen**.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung am Programm sieht vor, dass Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden, an Kaspersky Lab geschickt werden, außerdem ein einmaliger Identifikator, den Kaspersky Anti-Virus für Ihren Computer vergibt, sowie Systeminformationen. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich den Text für den Gebrauch von Kaspersky Security Network gründlich durch. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie das Häkchen im Kontrollkästchen ☒ **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

Klicken Sie auf **Weiter**. Die Installation wird fortgesetzt.

SCHRITT 6. INSTALLATIONSVERZEICHNIS AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn eine benutzerdefinierte Installation des Programms (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. [21](#)) gewählt wurde.

In dieser Phase der Installation wird Ihnen vorgeschlagen, den Ordner auf Ihrem Computer zu bestimmen, in den Kaspersky Anti-Virus installiert wird. Standardmäßig gilt folgender Pfad:

- <Datenträger> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2010 – für 32-bit-Systeme.
- <Datenträger> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2010 – für 64-bit-Systeme.

Sie können einen anderen Ordner angeben, indem Sie auf die Schaltfläche **Durchsuchen** klicken und Sie ihn im Standardfenster für die Ordnerauswahl vorgeben oder einen Pfad in das entsprechende Eingabefeld eintragen.

Beachten Sie: Wenn Sie ein komplettes Installationsverzeichnis manuell eingeben, darf es nicht länger als 200 Zeichen sein und keine Sonderzeichen enthalten.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. PROGRAMMKOMPONENTEN FÜR INSTALLATION AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn eine benutzerdefinierte Installation des Programms (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. [21](#)) gewählt wurde.

Bei der benutzerdefinierten Installation müssen die Komponenten von Kaspersky Anti-Virus definiert werden, die Sie auf Ihrem Computer installieren wollen. Standardmäßig werden für die Installation alle Komponenten von Kaspersky Anti-Virus ausgewählt: Schutzkomponenten, Untersuchungs- und Update-Aufgaben.

Um sich entscheiden zu können, welche Komponenten Sie nicht installieren wollen, sehen Sie sich die Kurzinformationen zur jeweiligen Komponente an. Gehen Sie dazu auf die Komponente in der Liste und lesen Sie im unten stehenden Feld den Text. Im Text werden kurz die Funktion der Komponente und der benötigte Speicherplatz auf dem Datenträger beschrieben.

Um die Installation einer Komponente abzulehnen, öffnen Sie das Kontextmenü auf dem Symbol neben dem Namen der Komponente und gehen Sie auf den Punkt **Die Komponente wird nicht verfügbar sein**. Beachten Sie, wenn Sie die Installation einer Komponente verwehren, werden Sie vor einer ganzen Reihe von gefährlichen Programmen nicht geschützt.

Um eine Komponente zur Installation auszuwählen, öffnen Sie das Kontextmenü auf dem Symbol neben dem Namen der Komponenten und gehen Sie auf den Punkt **Die Komponente wird auf der lokalen Festplatte installiert**.

Nachdem die zu installierenden Komponenten bestimmt worden sind, klicken Sie auf die Schaltfläche **Weiter**. Um zur Liste mit den standardmäßig zu installierenden Komponenten zurückzugehen, klicken Sie auf die Schaltfläche **Zurück**.

SCHRITT 8. PROGRAMMEINSTELLUNGEN EINER VORGÄNGERVERSION VERWENDEN

Auf dieser Etappe können Sie festlegen, ob bei der Arbeit des Programms die Schutzeinstellungen und Programm-Datenbanken verwendet werden sollen, wenn solche auf Ihrem Computer bei der Deinstallation einer älteren Version von Kaspersky Anti-Virus gespeichert wurden.

Es wird detailliert betrachtet, wie sich die oben beschriebenen Optionen nutzen lassen.

Wenn auf Ihrem Computer bereits eine ältere Version (Build) von Kaspersky Anti-Virus installiert war und bei der Deinstallation die Programm-Datenbanken auf dem Computer gespeichert wurden, können Sie diese in der zu installierenden Version verwenden. Setzen Sie dazu das Häkchen im Kontrollkästchen ☒ **Programm-Datenbanken**. Die ursprünglich mitgelieferten Datenbanken werden nicht auf Ihren Computer kopiert.

Um die Schutzparameter zu verwenden, die Sie in der vorherigen Version eingestellt und auf dem Computer gespeichert haben, aktivieren Sie das Kontrollkästchen ☒ **Funktionsparameter des Programms**.

SCHRITT 9. NACH ANDEREN ANTIVIREN-ANWENDUNGEN SUCHEN

In dieser Phase wird nach anderen auf Ihrem Computer installierten Antiviren-Produkten gesucht, darunter auch nach Kaspersky-Lab-Programmen, deren gemeinsame Verwendung mit Kaspersky Anti-Virus zu Konflikten führen könnte.

Beim Erkennen von solchen Programmen auf Ihrem Computer wird die Liste auf dem Bildschirm angezeigt. Ihnen wird deren Deinstallation vorgeschlagen, bevor Sie mit der Installation fortsetzen.

Unter der Liste mit den erkannten Antiviren-Programmen können Sie die Variante Deinstallation – automatisch oder manuell auswählen.

Wenn unter den erkannten Antiviren-Programmen auch ein Kaspersky-Lab-Programm mit der Version 2009 ist, empfohlen wird, bei dessen manueller Deinstallation die Schlüsseldatei dieses Programms zu speichern. Sie können den Schlüssel für das neue Programm weiter verwenden. Außerdem empfohlen wird, die Quarantäne- und Backup-Objekte zu speichern. Kaspersky Anti-Virus verschiebt sie automatisch in die Quarantäne der neuen Version und sie können damit weiter arbeiten.

Bei der automatischen Deinstallation eines Programms der Version 2009 speichert das Programm die Aktivierungsdaten und sie werden für die Installation der Version 2010 herangezogen.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 10. PROGRAMMINSTALLATION ABSCHLIEßEND VORBEREITEN

In dieser Phase wird Ihnen vorgeschlagen, die Vorbereitungen für die Installation von Kaspersky Anti-Virus auf Ihrem Computer abzuschließen.

Bei der erstmaligen und benutzerdefinierten Installation (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 21) des Programms wird nicht empfohlen, das Kontrollkästchen ☒ **Installationsprozess schützen** zu deaktivieren. Wenn während der Programminstallation ein Fehler auftritt, kann der eingeschaltete Schutz für ein korrektes Rollback der Installation sorgen. Bei einer wiederholten Installation kann das Häkchen im Kontrollkästchen entfernt werden.

Bei einer Remote-Installation des Programms auf dem Computer über *Windows Remote Desktop* wird empfohlen, das Häkchen im Kontrollkästchen ☒ **Installationsprozess schützen** zu entfernen. Wenn das Häkchen im Kontrollkästchen stehen sollte, kann der Installationsvorgang nicht oder nicht richtig ausgeführt werden.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Im Verlauf der Installation unterbrechen die Komponenten von Kaspersky Anti-Virus, die den Datenverkehr im Netzwerk abfangen, die vorhandenen Netzwerkverbindungen. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 11. INSTALLATIONSVORGANG ABSCHLIEßEN

Im Fenster **Installation fertig stellen** stehen Angaben über den Abschluss der Installation von Kaspersky Anti-Virus auf Ihrem Computer.

Im nächsten Schritt wird das Programm so konfiguriert, dass Ihre Daten auf dem Computer maximal geschützt werden. Kaspersky Anti-Virus lässt sich schnell und richtig mit dem Konfigurationsassistenten (s. Abschnitt "Konfigurationsassistent des Programms" auf S. [26](#)) einstellen.

Klicken Sie auf die Schaltfläche **Weiter**, um zur Konfiguration des Programms zu wechseln.

ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Anti-Virus bestand eine der Hauptaufgaben der Kaspersky-Lab-Spezialisten in der optimalen Konfiguration aller Programmeinstellungen. Das verleiht einem Benutzer unabhängig von seiner Erfahrung mit Computern die Möglichkeit, sofort nach der Programminstallation die Sicherheit des Computers zu gewährleisten, ohne sich weiter mit den Einstellungen zu beschäftigen.

Zur Vereinfachung haben wir versucht, die Voreinstellung auf einer einheitlichen Oberfläche des Konfigurationsassistenten des Programms (s. Abschnitt "Konfigurationsassistent des Programms" auf S. [26](#)) zusammenzufassen, der nach dem Installationsvorgang gestartet wird. Mit Unterstützung des Assistenten können Sie Kaspersky Anti-Virus aktivieren, die Updateparameter anpassen, den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken und andere Einstellungen vornehmen.

Es kann sein, dass Ihr Computer bereits von Schadprogrammen infiziert wurde, bevor Sie Kaspersky Anti-Virus installiert haben. Um bereits vorhandene Malware zu finden, starten Sie die Untersuchung des Computers.

Durch Aktionen schädlicher Programme und Systemabstürze können die Einstellungen Ihres Computers beschädigt werden. Starten Sie die Aufgabe Suche nach Schwachstellen (s. Abschnitt "Untersuchung des Computers auf Schwachstellen" auf S. [31](#)), um Schwachstellen des installierten Programms und Anomalien in den Systemeinstellungen zu finden.

Die im Lieferumfang enthaltenen Datenbanken können zum Zeitpunkt der Programminstallation veraltet sein. Starten Sie das Programm-Update (sofern das Update nicht mit Hilfe des Konfigurationsassistenten oder sofort nach der Installation automatisch erfolgt ist).

Die Programmkomponente Anti-Spam verwendet einen lernfähigen Algorithmus zum Erkennen unerwünschter E-Mails. Starten Sie den Trainingsassistenten für Anti-Spam, um die Komponente auf die Arbeit mit Ihren E-Mails einzustellen.

Nach den oben beschriebenen Aktionen ist Kaspersky Anti-Virus zur Arbeit bereit. Verwenden Sie den Assistenten zu Sicherheitsverwaltung, um das Schutzniveau Ihres Computers zu beurteilen.

IN DIESEM ABSCHNITT

Konfigurationsassistent des Programms	26
Programm-Update	30
Virenuntersuchung des Computers	31
Untersuchung des Computers auf Schwachstellen	31
Lizenzverwaltung	31
Teilnahme an Kaspersky Security Network	32
Sicherheitsverwaltung	33
Schutzstatus	35
Schutz anhalten	35

KONFIGURATIONSSASSISTENT DES PROGRAMMS

Der Konfigurationsassistent für das Programm wird am Ende der Installation gestartet. Seine Aufgabe ist es, Sie bei der ersten Konfiguration der Parameter für Kaspersky Anti-Virus zu unterstützen und dabei die Besonderheiten der Aufgaben Ihres Computers zu berücksichtigen.

Der Konfigurationsassistent besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltfläche **Zurück** und der Link **Weiter**. Der Assistent wird mit Hilfe der Schaltfläche **Abbrechen** abgeschlossen.

DETAILS ZU DEN EINZELNEN SCHRITTEN DES ASSISTENTEN

Schritt 1. Programm aktivieren	27
Schritt 2. Schutzmodus auswählen	28
Schritt 3. Programm-Update anpassen	29
Schritt 4. Kontrolle des Zugriffs auf das Programm	29
Schritt 5. Erkennbare Bedrohungen auswählen	30
Schritt 6. Assistenten abschließen	30

SCHRITT 1. PROGRAMM AKTIVIEREN

Bei der Programmaktivierung wird durch die Installation eines Aktivierungscodes eine Lizenz registriert. Auf Grundlage der Lizenz ermittelt das Programm, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer dafür gilt.

Der Schlüssel enthält Dienstinformationen, die für die volle Funktionsfähigkeit von Kaspersky Anti-Virus erforderlich sind, sowie zusätzliche Angaben:

- Informationen über den Support (von wem und wo man technische Unterstützung erhalten kann).
- Bezeichnung, Nummer und Gültigkeitsdauer der Lizenz.

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Um bei der Aktivierung eine Schlüsseldatei zu erhalten, ist ein Aktivierungscode erforderlich. Einen Aktivierungscode erhalten Sie beim Kauf des Programms. Für die Aktivierung von Kaspersky Anti-Virus bestehen folgende Möglichkeiten:

- **Kommerzielle Version aktivieren.** Wählen Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben und Sie einen Aktivierungscode erhalten haben. Auf Basis dieses Codes bekommen Sie eine Schlüsseldatei, die Ihnen während der gesamten Laufzeit der Lizenz den Zugriff auf die volle Funktionsfähigkeit des Programms bietet.
- **Testversion aktivieren.** Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten eine kostenlose Schlüsseldatei, deren Gültigkeitsdauer durch die Lizenz der Testversion dieses Programms beschränkt ist.
- **Später aktivieren.** Bei der Auswahl dieser Variante wird die Aktivierung von Kaspersky Anti-Virus übersprungen. Das Programm wird auf Ihrem Computer installiert und Sie können alle Programmfunktionen außer dem Update nutzen (Kaspersky Anti-Virus kann nach der Installation nur einmal aktualisiert werden.) Die Variante **Später aktivieren** steht nur zur Verfügung, wenn der Aktivierungsassistent zum ersten Mal gleich nach der Programminstallation gestartet wird.

Wenn Kaspersky Anti-Virus früher installiert und dann gelöscht wurde, wobei die Informationen über die Aktivierung gespeichert wurden, dann fehlt dieser Schritt. In diesem Fall erhält der Konfigurationsassistent automatisch die Informationen über die vorhandene Lizenz, die im Fenster des Assistenten (s. S. [28](#)) angezeigt werden.

SIEHE AUCH

Kommerzielle Version aktivieren	28
Testversion aktivieren.....	28
Aktivierung abschließen	28

KOMMERZIELLE VERSION AKTIVIEREN

Wenn diese Variante gewählt wird, erfolgt die Programmaktivierung über den Webserver von Kaspersky Lab. Dafür ist eine Internetverbindung erforderlich.

Die Aktivierung beruht auf der Eingabe des Aktivierungscodes, den Sie per E-Mail erhalten, wenn Sie Kaspersky Anti-Virus über das Internet kaufen. Wenn Sie das Programm in einer DVD-Box kaufen, steht der Aktivierungscode auf der Innenseite des DVD-Umschlags oder unter einer Schutzschicht des Aufklebers auf der Innenseite der DVD-Box.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Ziffernfolge mit vier Blöcken zu je fünf Ziffern ohne Leerzeichen. Zum Beispiel 11111-11111-11111-11111. Beachten Sie bitte, dass der Code in lateinischen Buchstaben eingegeben werden muss.

Der Aktivierungsassistent baut eine Verbindung mit dem Kaspersky-Lab-Aktivierungsserver im Internet auf und sendet Ihren Aktivierungscode an den Server, der den Code überprüft. Wenn der Aktivierungscode die Überprüfung besteht, erhält der Assistent eine Schlüsseldatei, die automatisch installiert wird. Der Aktivierungsvorgang wird abgeschlossen und auf dem Bildschirm erscheint ein Fenster mit ausführlichen Informationen über die erworbene Lizenz.

Wenn der Aktivierungscode die Überprüfung nicht bestanden hat, erscheint eine entsprechende Meldung auf dem Bildschirm. In diesem Fall sollten Sie sich an die Firma wenden, bei der Sie Kaspersky Anti-Virus gekauft haben.

Wenn die zulässige Anzahl der Aktivierungen für diesen Aktivierungscode überschritten wurde, erscheint eine entsprechende Meldung auf dem Bildschirm. Der Aktivierungsvorgang wird abgebrochen und das Programm schlägt Ihnen vor, sich an den Support von Kaspersky Lab zu wenden.

Wenn bei Verbindung mit dem Aktivierungsserver Fehler eingetreten sind und keine Schlüsseldatei heruntergeladen wurde, wenden Sie sich an den technischen Support.

TESTVERSION AKTIVIEREN

Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion von Kaspersky Anti-Virus installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Schlüssel, dessen Gültigkeitsdauer durch den Lizenzvertrag der Testversion des Programms beschränkt ist. Nach Ablauf der Probelizenz ist es nicht möglich, eine weitere Probelizenz zu aktivieren.

Wenn bei Verbindung mit dem Aktivierungsserver Fehler eingetreten sind und keine Schlüsseldatei heruntergeladen wurde, wenden Sie sich an den technischen Support.

AKTIVIERUNG ABSCHLIEßEN

Der Aktivierungsassistent informiert Sie über den erfolgreichen Abschluss der Aktivierung von Kaspersky Anti-Virus. Außerdem werden Informationen über die Lizenz angezeigt: Typ (kommerziell, Test usw.), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

SCHRITT 2. SCHUTZMODUS AUSWÄHLEN

Wählen Sie einen Modus für den Schutz, der von Kaspersky Anti-Virus gewährleistet wird.

Es stehen zwei Modi zur Auswahl:

- *Automatisch.* Beim Eintreten wichtiger Ereignisse führt Kaspersky Anti-Virus automatisch die Aktion aus, die von den Kaspersky-Lab-Spezialisten empfohlen wird. Beim Fund einer Bedrohung versucht das Programm, das Objekt zu desinfizieren, und wenn die Desinfektion fehlschlägt, wird das Objekt gelöscht. Verdächtige Objekte werden unbearbeitet übersprungen. Über eingetretene Ereignisse wird durch Popupmeldungen informiert.
- *Interaktiv.* In diesem Modus reagiert das Programm so auf eintretende Ereignisse, wie Sie es festlegen. Beim Eintreten von Ereignissen, die Ihre Reaktion erfordern, zeigt das Programm eine Meldung (auf S. [133](#)), in der eine Aktion gewählt werden kann.

Meldungen über den Fund einer aktiven Infektion werden unabhängig davon angezeigt, welcher Schutzmodus gewählt wurde.

SCHRITT 3. PROGRAMM-UPDATE ANPASSEN

Dieser Schritt des Konfigurationsassistenten wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Die Qualität des Schutzes Ihres Computers ist unmittelbar vom rechtzeitigen Download der Updates für die Datenbanken und Programm-Module abhängig. In diesem Fenster des Assistenten können Sie den Modus für das Update von Kaspersky Anti-Virus auswählen und Einstellungen für den Zeitplan vornehmen:

- **Automatisches Update.** Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates gefunden werden, lädt das Programm sie herunter und installiert sie auf dem Computer. Dieser Modus wird standardmäßig verwendet.
- **Update nach Zeitplan** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Einstellungen** geöffnet wird.
- **Manuelles Update.** In diesem Fall starten Sie das Programm-Update manuell.

Beachten Sie, dass die Datenbanken und Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Installation von Kaspersky Anti-Virus bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Updates für Kaspersky Anti-Virus herunterzuladen. Klicken Sie dazu auf die Schaltfläche **Jetzt aktualisieren**. In diesem Fall empfängt das Programm die erforderlichen Updates von den Updateseiten im Internet und installiert sie auf Ihrem Computer.

Wenn die im Lieferumfang enthaltenen Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Wenn Sie die Updateparameter anpassen möchten (s. Abschnitt "Update" auf S. [87](#)) (die Quelle wählen, von der das Update erfolgt; den Start des Updates mit den Rechten eines bestimmten Benutzerkontos anzupassen; den Dienst zum Kopieren von Updates in eine lokale Quelle aktivieren), klicken Sie auf die Schaltfläche **Einstellungen**.

SCHRITT 4. KONTROLLE DES ZUGRIFFS AUF DAS PROGRAMM

Dieser Schritt des Konfigurationsassistenten von Kaspersky Anti-Virus wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Da ein PC von mehreren Personen verwendet werden kann, die über ein unterschiedliches Maß an Fertigkeiten im Umgang mit Computern verfügen, und weil Schadprogramme versuchen können, den Schutz Ihres Computers auszuschalten, wird Ihnen angeboten, den Zugriff auf Kaspersky Anti-Virus mit Hilfe eines Kennworts zu beschränken.

Das Kennwort erlaubt es, das Programm vor Versuchen zum unerlaubten Ausschalten des Schutzes oder zum Ändern der Einstellungen von Kaspersky Anti-Virus zu schützen.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen ☒ **Kennwortschutz aktivieren** und füllen Sie die Felder **Neues Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung beziehen soll:

- ☒ **Programmparameter ändern** – Kennwortabfrage beim Versuch des Benutzers, geänderte Einstellungen von Kaspersky Anti-Virus zu speichern.
- ☒ **Programm beenden** – Kennwortabfrage beim Versuch des Benutzers, die Arbeit des Programms zu beenden.

SCHRITT 5. ERKENNBARE BEDROHUNGEN AUSWÄHLEN

Dieser Schritt des Konfigurationsassistenten wird übersprungen, wenn der Modus zur schnellen Installation gewählt wurde. Die Programmparameter, die bei diesem Schritt angepasst werden, erhalten Standardwerte.

Auf dieser Etappe können Sie die Kategorien der Bedrohungen auswählen, vor denen Kaspersky Anti-Virus Ihren Computer schützen soll. Programme, die Ihrem Computer Schaden zufügen können, werden immer von Kaspersky Anti-Virus überwacht. Dazu gehören die Programmtypen Viren, Würmer und trojanische Programme.

SCHRITT 6. ASSISTENTEN ABSCHLIEßEN

Das letzte Fenster des Assistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky Anti-Virus zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen ☒ **Kaspersky Anti-Virus starten** aktiviert ist, und klicken Sie auf die Schaltfläche **Beenden**.

PROGRAMM-UPDATE

Für das Update von Kaspersky Anti-Virus ist eine bestehende Internetverbindung erforderlich.

Zum Lieferumfang von Kaspersky Anti-Virus gehören Datenbanken mit Bedrohungssignaturen. Zum Zeitpunkt der Installation von Kaspersky Anti-Virus können die Datenbanken veraltet sein, weil die Datenbanken und Programm-Module regelmäßig von Kaspersky Lab aktualisiert werden.

Im Verlauf des Konfigurationsassistenten des Programms können Sie den Startmodus für Update (s. Abschnitt "Schritt 3. Programm-Update anpassen" auf S. 29) auswählen. Kaspersky Anti-Virus überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Updateservern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, führt Kaspersky Anti-Virus im Hintergrundmodus den Download und die Installation der Updates durch.

Wenn die im Lieferumfang enthaltenen Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Um den Schutz Ihres Computers aktuell zu halten, wird empfohlen, Kaspersky Anti-Virus sofort nach der Installation zu aktualisieren.

➡ Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus auf Befehl zu aktualisieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie auf die Schaltfläche **Update ausführen**.

VIRENUNTERSUCHUNG DES COMPUTERS

Die Autoren schädlicher Programme strengen sich sehr an, die Aktivität ihrer Programme zu verheimlichen. Deshalb kann es sein, dass Sie die Existenz von Malware auf Ihrem Computer nicht bemerken.

Bei der Installation von Kaspersky Anti-Virus wird automatisch die Aufgabe **Schnelle Untersuchung** ausgeführt. Diese Aufgabe dient der Suche und Neutralisierung von schädlichen Programmen in Objekten, die beim Hochfahren des Betriebssystems geladen werden.

Die Spezialisten von Kaspersky Lab empfehlen, zusätzlich die Aufgabe **Vollständige Untersuchung** auszuführen.

➤ *Gehen Sie folgendermaßen vor, um eine Untersuchungsaufgabe zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche **Vollständige Untersuchung ausführen**, um die Untersuchung zu starten.

UNTERSUCHUNG DES COMPUTERS AUF SCHWACHSTELLEN

Aufgrund unerwünschter Aktivität auf Ihrem Computer, die durch Systemabstürze oder Aktivität schädlicher Programme verursacht werden kann, können den Einstellungen des Betriebssystems falsche Werte zugewiesen werden. Außerdem können auf Ihrem Computer installierte Programme Schwachstellen aufweisen, die Angreifern dazu dienen können, um Ihren Computer zu beschädigen.

Um derartige Sicherheitsprobleme zu erkennen und zu beheben, empfehlen die Kaspersky-Lab-Spezialisten, nach der Installation des Programms die *Aufgabe zur Suche nach Schwachstellen* (s. S. [82](#)) zu starten. Im Verlauf der Aufgabenausführung wird in den installierten Programmen nach Schwachstellen und in den Einstellungen des Betriebssystems und des Browsers nach Beschädigungen und Anomalien gesucht.

➤ *Gehen Sie folgendermaßen vor, um die Aufgabe zur Schwachstellen-Suche zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche **Fenster zur Suche nach Schwachstellen öffnen**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Suche nach Schwachstellen ausführen**.

LIZENZVERWALTUNG

Die Möglichkeit zur Benutzung von Kaspersky Anti-Virus wird durch das Vorhandensein einer Schlüsseldatei bestimmt. Eine Schlüsseldatei erhalten Sie mit Hilfe des Aktivierungscodes, der Ihnen beim Kauf des Programms zur Verfügung gestellt wird. Sie berechtigt Sie ab dem Tag der Aktivierung zur Nutzung des Programms. Der Schlüssel enthält Informationen zur Lizenz: Typ, Gültigkeitsdauer und Anzahl der Computer, für die die Lizenz gültig ist.

Wenn kein Schlüssel vorhanden ist und keine Testversion von Kaspersky Anti-Virus aktiviert wurde, wird das Programm in einem Modus funktionieren, in dem das Update nur ein einziges Mal möglich ist. Danach werden keine neuen Updates mehr ausgeführt.

Wenn eine Testversion des Programms aktiviert wurde, wird Kaspersky Anti-Virus nach dem Ablauf der Nutzungsdauer nicht mehr funktionieren.

Bei Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz bleibt die Funktionalität des Programms unter Ausnahme der Updatemöglichkeit für die Programm-Datenbanken erhalten. Sie können Ihren Computer mit Hilfe der Untersuchungsaufgaben weiterhin untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Datenbanken, die bei Ablauf der Lizenz aktuell waren. Demzufolge können wir Ihnen keinen maximalen Schutz vor neuen Viren garantieren, die nach dem Gültigkeitsende der Lizenz gefunden werden.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wir Ihnen, die Lizenz für die Benutzung von Kaspersky Anti-Virus zu verlängern. Zwei Wochen vor Gültigkeitsende der Lizenz werden Sie vom Programm darüber benachrichtigt. Innerhalb eines bestimmten Zeitraums wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Informationen über die aktive Lizenz befinden sich im Fenster des **Lizenz-Managers**: Typ (kommerziell, Test), maximale Anzahl der Computer, auf denen diese Lizenz verwendet werden darf, Gültigkeitsdauer und Anzahl der bis zum Ablauf verbleibenden Tage.

Zu den Bedingungen des Lizenzvertrags über die Nutzung des Programms gelangen Sie über die Schaltfläche **Lizenzvertrag lesen**. Um eine Schlüsseldatei zu löschen, klicken Sie auf die Schaltfläche **X**, die sich rechts von der Lizenz befindet, deren Schlüsseldatei gelöscht werden soll. Um eine neue Lizenz zu aktivieren, verwenden Sie die Schaltfläche **Neue Lizenz aktivieren**.

Mit Hilfe der Schaltfläche **Lizenz kaufen (Lizenz verlängern)** können Sie zum Kauf (Verlängerung) einer Lizenz in den Online-Shop von Kaspersky Lab gehen.

Kaspersky Lab führt in regelmäßigen Zeitabständen Aktionen durch, bei denen Lizenzen für unsere Produkte zu besonders günstigen Preisen angeboten werden. Verfolgen Sie unsere Aktionen auf der Internetseite von Kaspersky Lab.

TEILNAHME AN KASPERSKY SECURITY NETWORK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um das Erstellen einer Statistik über neue Bedrohungstypen und ihre Quellen sowie die Entwicklung entsprechender Neutralisierungsmethoden zu beschleunigen, bietet Kaspersky Lab Ihnen die Teilnahme an dem Dienst Kaspersky Security Network an.

Bei der Verwendung von Kaspersky Security Network werden folgende Informationen an Kaspersky Lab gesendet:

- Unikatler Identifikator, den das Kaspersky Anti-Virus Ihrem Computer zugewiesen hat. Dieser Identifikator charakterisiert die Hardwareparameter Ihres Computers und enthält keinerlei persönliche Informationen.
- Informationen über die Bedrohungen, die von den Programmkomponenten gefunden wurden. Die Auswahl der Informationen ist vom Typ der gefundenen Bedrohung abhängig.
- Informationen über das System: Version des Betriebssystems, installierte Service Packs, geladene Dienste und Treiber, Versionen von Browsern und Mailprogrammen, Erweiterungen für Browser, Versionsnummer des installierten Kaspersky-Lab-Programms.

Im Rahmen von Kaspersky Security Network wird außerdem eine erweiterte Statistik erstellt. Dazu gehören Informationen über:

- auf Ihrem Computer geladene ausführbare Dateien und signierte Programme.
- auf Ihrem Computer gestartete Programme.

Die statistischen Informationen werden bei Abschluss des Programm-Updates gesendet.

Kaspersky Lab garantiert, dass im Rahmen von Kaspersky Security Network keine persönlichen Benutzerdaten gesammelt und gesendet werden.

➡ Gehen Sie folgendermaßen vor, um Parameter für das Senden einer Statistik anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Feedback**.
3. Aktivieren Sie das Kontrollkästchen ☒ **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**, um die Teilnahme an Kaspersky Security Network zu bestätigen.

SICHERHEITSVERWALTUNG

Auftretende Probleme beim Schutz des Computers signalisiert der Schutzstatus des Computers (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)): Es ändert sich die Farbe des Schutzstatus-Symbols auch in der Leiste, wo es angezeigt wird. Wenn im Schutz Probleme auftreten, sollten diese umgehend behoben werden.



Abbildung 1. Aktueller Schutzstatus des Computers

Durch Klick auf das Symbol für den Status oder auf die Leiste, auf der sich das Symbol befindet (s. Abbildung oben), gelangen Sie auf die Registerkarte **Status** (s. Abbildung unten), die eine Liste der aufgetretenen Probleme enthält und entsprechende Lösungsmöglichkeiten bietet.

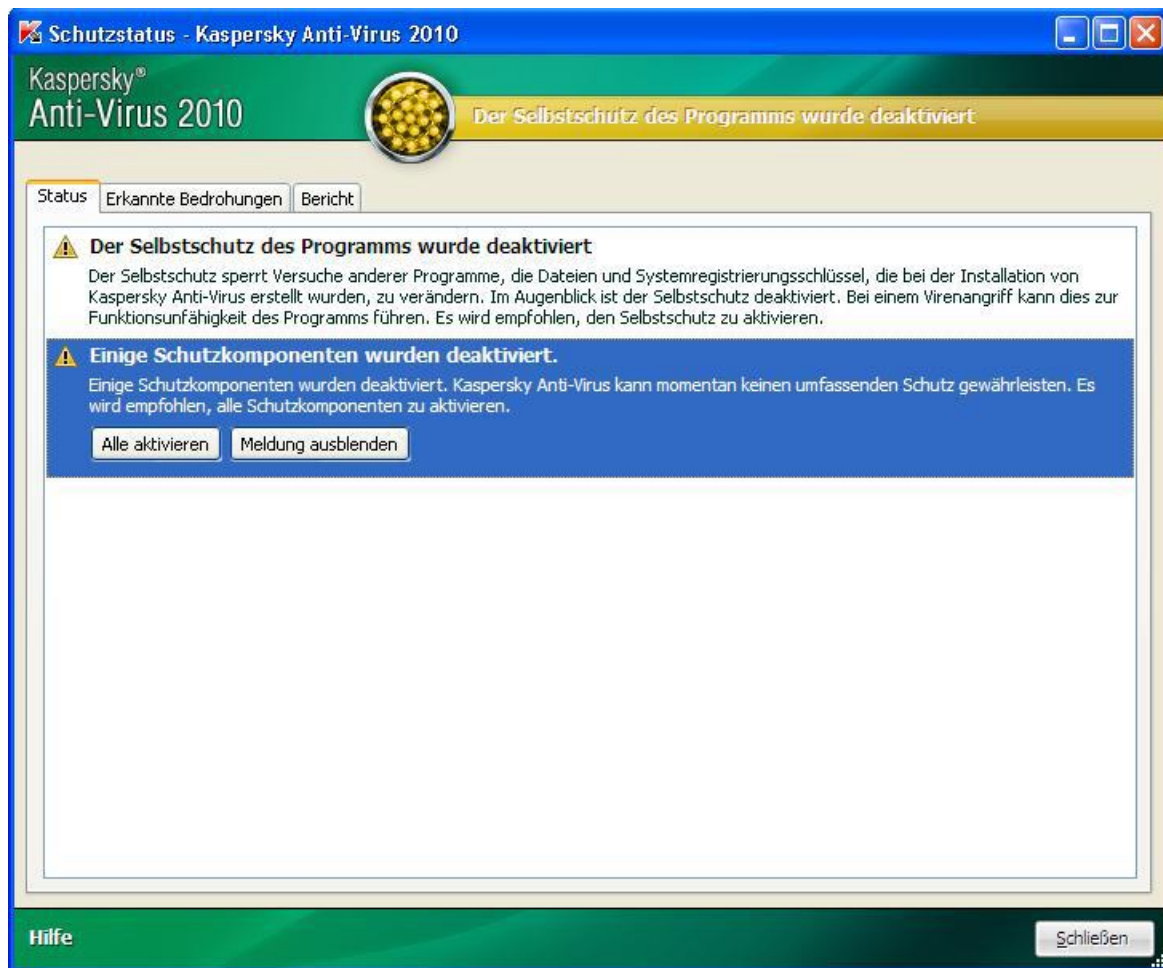


Abbildung 2. Sicherheitsprobleme beheben

Sie können eine Liste der vorhandenen Probleme ansehen. Die Probleme sind ihrer Priorität entsprechend angeordnet und sollten in dieser Reihenfolge gelöst werden: Zu Beginn stehen die wichtigsten Probleme, die mit einem rotem Symbol gekennzeichnet sind, danach die weniger wichtigen mit gelbem Symbol und zum Schluss informative Meldungen. Für jedes Problem ist eine ausführliche Beschreibung vorhanden und folgende Aktionen werden angeboten:

- **Sofort beheben.** Mit Hilfe der entsprechenden Schaltflächen können Sie zur sofortigen Neutralisierung der Probleme übergehen, was der empfohlenen Aktion entspricht.
- **Behebung aufschieben.** Wenn das sofortige Beheben eines Problems aufgrund bestimmter Umstände nicht möglich ist, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Klicken Sie dazu auf die Schaltfläche **Meldung ausblenden**.

Beachten Sie, dass diese Möglichkeit für kritische Probleme nicht vorgesehen ist. Dazu gehören beispielsweise die Existenz nicht neutralisierter schädlicher Objekte, Störungen bei der Arbeit einer oder mehrerer Komponenten, und beschädigte Programmdateien.

Um Meldungen, die zuvor ausgeblendet wurden, erneut in der Liste anzuzeigen, aktivieren Sie das Kontrollkästchen ☒ **Ausgeblendete Meldungen anzeigen**.

SCHUTZSTATUS

Die Arbeit der Komponenten von Kaspersky Anti-Virus oder der Untersuchungsaufgaben wird im Bericht dokumentiert, der Informationen über den Zustand des Computerschutzes enthält. Hier können Sie erfahren, wie viele gefährliche und verdächtige Objekte das Programm gefunden hat und welche dieser Objekte desinfiziert, gelöscht oder in die Quarantäne verschoben worden sind.

Wenn das Programm schädliche Objekte gefunden hat, wird dies durch den Schutzstatus des Computers signalisiert (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. 39), indem sich die Farbe des Schutzstatussymbols und der Leiste, auf der sich das Symbol befindet, verändert. Beim Fund schädlicher Objekte ändert sich die Farbe des Symbols und der Leiste in Rot. In diesem sollten alle vorhandenen Bedrohungen umgehend neutralisiert werden.

➡ *Gehen Sie folgendermaßen vor, um sich über den Zustand des Computerschutzes zu informieren:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Link **Bericht**.

➡ *Gehen Sie folgendermaßen vor, um im Computerschutz vorhandene Probleme zu beheben:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Link **Bericht**.
3. Führen Sie im folgenden Fenster auf der Registerkarte **Status** die entsprechenden Aktionen aus. Um Meldungen, die zuvor ausgeblendet wurden, erneut in der Liste anzuzeigen, aktivieren Sie das Kontrollkästchen ☒ **Ausgeblendete Meldungen anzeigen**.

➡ *Gehen Sie folgendermaßen vor, um eine Aktion mit einem gefundenen Objekt auszuführen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Link **Bericht**.
3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** in der Liste das entsprechende Objekt aus und öffnen Sie durch Rechtsklick sein Kontextmenü.
4. Wählen Sie im Kontextmenü die erforderliche Aktion aus.

➡ *Gehen Sie folgendermaßen vor, um einen Bericht über die Arbeit der Schutzkomponenten zu lesen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Link **Bericht**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Bericht** aus.

SCHUTZ ANHALTEN

Das Anhalten des Schutzes bedeutet, dass alle Komponenten für einen bestimmten Zeitraum ausgeschaltet werden.

Durch das vorübergehende Deaktivieren wird die Arbeit aller Schutzkomponenten angehalten. Darüber informieren:

- Das inaktive (graue) Programmsymbol (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 37) im Infobereich der Taskleiste;
- Rote Farbe von Statussymbol und Leiste im Hauptfenster von Kaspersky Anti-Virus.

Wenn im Augenblick, als der Schutz beendet wurde, auf dem Computer Netzwerkverbindungen aktiv waren, erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt werden.

➡ Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:

1. Im Kontextmenü (s. Abschnitt "Kontextmenü" auf S. [38](#)) des Programms wählen Sie den Punkt **Schutz anhalten**.
2. Wählen Sie im folgenden Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
 - **Anhalten für <Zeitintervall>** - Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert. Wählen Sie in der Dropdown-Liste einen Wert für den Zeitraum aus.
 - **Anhalten bis zum Neustart** – Der Schutz wird nach dem Neustart des Programms oder des Systems aktiviert (unter der Bedingung, dass die Funktion zum Start von Kaspersky Anti-Virus beim Hochfahren des Systems aktiviert ist).
 - **Anhalten** – Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz fortsetzen** im Kontextmenü des Programms, um den Schutz zu aktivieren.

PROGRAMMOBERFLÄCHE

Kaspersky Anti-Virus bietet eine intuitive bedienbare und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben.

Kaspersky Anti-Virus verfügt über Erweiterungskomponenten (Plug-ins), die in folgende Programme integriert werden können: Microsoft Office Outlook, The Bat!, Microsoft Internet Explorer, Microsoft Windows Explorer. Die Plug-ins erweitern die Möglichkeiten der genannten Programme, weil die Konfiguration der Komponenten direkt aus ihrer Programmoberfläche möglich ist.

IN DIESEM ABSCHNITT

Symbol im Infobereich der Taskleiste	37
Kontextmenü	38
Hauptfenster von Kaspersky Anti-Virus	39
Meldungen.....	41
Programmkonfigurationsfenster	41

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach der Installation von Kaspersky Anti-Virus erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol dient als Indikator für die Arbeit des Programms. Es informiert über den Schutzstatus und zeigt eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

Wenn das Symbol aktiv  (farbig) ist, bedeutet es, dass der Schutz vollständig aktiviert ist oder bestimmte Schutzkomponenten aktiv sind. Wenn das Symbol inaktiv  (schwarzweiß) ist, dann wurden alle Schutzkomponenten deaktiviert.

Je nach der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Anti-Virus:



– Die Untersuchung einer E-Mail-Nachricht wird ausgeführt.



– Die Untersuchung des Web-Datenverkehrs wird ausgeführt.



– Das Update der Datenbanken und der Programm-Module wird ausgeführt.



– Der Neustart des Computers ist erforderlich, um die Updates zu übernehmen.



– Bei der Arbeit einer Programmkomponente ist eine Störung aufgetreten.

Außerdem sorgt das Symbol für den Zugang zu den Grundelementen der Programmoberfläche: Kontextmenü (s. Abschnitt "Kontextmenü" auf S. [38](#)) und Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)).

Das Kontextmenü wird durch Rechtsklick auf das Programmsymbol geöffnet.

Um das Hauptfenster von Kaspersky Anti-Virus zu öffnen, klicken Sie mit der linken Maustaste auf das Programmsymbol.

Wenn Neuigkeiten von Kaspersky Lab erschienen sind, wird im Infobereich der Taskleiste von Microsoft Windows das Symbol  eingeblendet. Der Nachrichtentext wird durch Doppelklick auf das entsprechende Symbol geöffnet.

KONTEXTMENÜ

Das Kontextmenü bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü von Kaspersky Anti-Virus enthält folgende Punkte:

- **Update** - Starten der Aktualisierung der Datenbanken und Module des Programms und der Installation der Updates auf Ihrem Computer.
- **Computer vollständig untersuchen** – Starten der vollständigen Untersuchung Ihres Computers auf das Vorhandensein schädlicher Objekte. Dabei werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.
- **Auf Viren untersuchen** - Zur Auswahl von Objekten und zum Start der Virensuche wechseln. In der Grundeinstellung enthält die Liste eine Reihe von Objekten wie beispielsweise den Ordner **Eigene Dateien** und Mailboxen. Sie können die Liste ergänzen, Untersuchungsobjekte auswählen und die Virensuche starten.
- **Virtuelle Tastatur** - zu der virtuellen Tastatur wechseln.
- **Kaspersky Anti-Virus** – Öffnen des Programmhauptfensters (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)).
- **Einstellungen** – Zur Anzeige und Konfiguration der Funktionsparameter des Programms wechseln.
- **Aktivierung** – Wechsel zur Aktivierung von Kaspersky Anti-Virus. Um den Status eines registrierten Benutzers zu erhalten, muss Ihre Version des Programms aktiviert werden. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.
- **Über das Programm** – Informationsfenster aufrufen, in dem Programminformationen angezeigt werden.
- **Schutz anhalten / Schutz fortsetzen** – zeitweises Ausschalten / Einschalten von Komponenten des Echtzeitschutzes. Dieser Menüpunkt bezieht sich nicht auf das Programm-Update und die Ausführung von Aufgaben zur Virensuche.
- **Beenden** – Arbeit von Kaspersky Anti-Virus beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entfernt).



Abbildung 3. Kontextmenü

Wird das Kontextmenü geöffnet, während eine Aufgabe zur Virensuche läuft, so wird ihr Name mit Prozentangabe des Ausführungsergebnisses im Kontextmenü angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Hauptfenster mit dem Bericht über ihre aktuellen Ausführungsergebnisse.

HAUPTFENSTER VON KASPERSKY ANTI-VIRUS

Das Programmhauptfenster lässt sich bedingt in drei Bereiche aufteilen:

- Der obere Bereich des Fensters informiert über den aktuellen Schutzstatus Ihres Computers.



Abbildung 4. Aktueller Schutzstatus des Computers

Es gibt drei Varianten für den Schutzstatus. Jeder Status wird durch eine bestimmte Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Die Farbe Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass bestimmte Sicherheitsbedrohungen vorliegen. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, die deaktivierten Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

Vorhandene Sicherheitsrisiken sollten umgehend behoben werden. Um ausführliche Informationen darüber zu erhalten und die Bedrohungen schnell zu beheben, verwenden Sie den Assistenten zu Sicherheitsverwaltung oder klicken Sie auf das Symbol für den Status oder für die Leiste, auf der sich das Symbol befindet (s. Abbildung oben).

- Die linke Seite des Fensters bietet schnellen Zugriff auf alle Programmfunktionen, auf die Ausführung von Aufgaben zur Virensuche oder zum Update, u.a.



Abbildung 5. Linke Seite des Hauptfensters

- Die rechte Seite des Fensters enthält Informationen über die auf der linken Seite ausgewählte Programmfunktion, erlaubt es, ihre Parameter anzupassen, bietet Werkzeuge zum Ausführen von Aufgaben zur Virensuche, zum Update-Download, u.a.



Abbildung 6. Rechte Seite des Hauptfensters

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- Einstellungen** – in das Programmkonfigurationsfenster wechseln (s. Abschnitt "Konfiguration des Programms" auf S. 93).
- Quarantäne** – zur Arbeit mit Objekten, die in die Quarantäne verschoben wurden, wechseln.
- Bericht** – zu einer Liste der Ereignisse, die bei der Arbeit des Programms eingetreten sind, wechseln.
- Hilfe** – zum Hilfesystem für Kaspersky Anti-Virus wechseln.
- Mein Kaspersky Account** – in den persönlichen Bereich des Benutzers auf der Seite des Technischen Supports gehen.
- Support** – Das Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (Webseite des technischen Supports, Forum) öffnen.
- Lizenz** – Zur Aktivierung von Kaspersky Anti-Virus bzw. zur Verlängerung der Lizenzgültigkeitsdauer wechseln.

Sie können das Aussehen von Kaspersky Anti-Virus verändern, indem Sie grafische Elemente und Farbschemen erstellen und verwenden.

MELDUNGEN

Wenn bei der Arbeit von Kaspersky Anti-Virus bestimmte Ereignisse eintreten, werden Sie durch Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows darüber informiert.

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm.** Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: Ein Virus wurde gefunden oder im System wurde gefährliche Aktivität erkannt. Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Meldungen dieses Typs sind rot gekennzeichnet.
- **Warnung.** Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Sie werden aufgefordert, über die Gefährlichkeit dieses Ereignisses zu entscheiden. Meldungen dieses Typs sind gelb gekennzeichnet.
- **Info.** Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Informative Meldungen dieses Typs sind grün gekennzeichnet.

SIEHE AUCH

Meldungen.....[133](#)

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster für die Einstellung von Kaspersky Anti-Virus lässt sich aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)) oder aus dem Kontextmenü (s. Abschnitt "Kontextmenü" auf S. [38](#)) öffnen. Klicken Sie dazu im oberen Bereich des Hauptfensters auf den Link **Einstellungen** oder wählen Sie den gleichnamigen Punkt im Kontextmenü des Programms aus.

Das Konfigurationsfenster besteht aus zwei Teilen:

- Die linke Seite des Fensters bietet Zugriff auf die Funktionen von Kaspersky Anti-Virus, auf Untersuchungs- und Updateaufgaben usw.
- Die rechte Seite des Fensters enthält eine Liste von Parametern für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

SCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS

Datei-Anti-Virus erlaubt es, das Dateisystem des Computers vor einer Infektion zu schützen. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

In der Grundeinstellung untersucht Datei-Anti-Virus nur neue oder veränderte Dateien. Die Untersuchung von Dateien erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Beim Fund von Bedrohungen führt Datei-Anti-Virus die festgelegte Aktion aus.

Das Schutzniveau für die Dateien und den Speicher auf Ihrem Computer wird durch folgende Gruppen von Parametern definiert:

- Parameter, die den Schutzbereich festlegen.
- Parameter, die die verwendete Untersuchungsmethode festlegen.
- Parameter, die die Untersuchung von zusammengesetzten Dateien (einschließlich der Untersuchung umfangreicher zusammengesetzter Dateien) festlegen.
- Parameter, die den Untersuchungsmodus festlegen.
- Parameter, die es erlauben, die Arbeit der Komponente nach Zeitplan oder während der Arbeit bestimmter Programme anzuhalten.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Datei-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, die Sicherheitsstufe zu ändern. Sie können die Standardeinstellungen von Datei-Anti-Virus wiederherstellen. Wählen Sie dazu eine Sicherheitsstufe aus.

➡ Gehen Sie folgendermaßen vor, um die Funktionsparameter von Datei-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente	43
Sicherheitsstufe für Dateien und Speicher ändern	44
Aktion für gefundene Objekte ändern	44
Schutzbereich festlegen	45
Heuristische Analyse verwenden	46
Untersuchung optimieren	47
Untersuchung von zusammengesetzten Dateien	47
Untersuchung umfangreicher zusammengesetzter Dateien	47
Untersuchungsmodus ändern	48
Untersuchungstechnologie	48
Komponente anhalten: Zeitplan erstellen	49
Komponente anhalten: Liste der Programme erstellen	50
Standardmäßige Schutzparameter wiederherstellen	51

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Datei-Anti-Virus wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

Standardmäßig untersucht Datei-Anti-Virus nur neue oder veränderte Dateien, d.h. Dateien, die seit dem letzten Zugriff hinzugefügt oder verändert wurden. Die Untersuchung einer Datei erfolgt nach folgendem Algorithmus:

1. Die Komponente fängt den Zugriff des Benutzers oder eines bestimmten Programms auf eine beliebige Datei ab.
2. Datei-Anti-Virus prüft, ob in den Datenbanken iChecker und iSwift Informationen über die abgefangene Datei vorhanden sind. Auf Basis dieser Informationen wird entschieden, ob eine Untersuchung der Datei erforderlich ist.

Bei der Untersuchung werden folgende Aktionen ausgeführt:

1. Die Datei wird auf das Vorhandensein von Viren untersucht. Das Erkennen von Objekten erfolgt auf Basis der Datenbanken von Kaspersky Ant-Virus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten Schadprogramme, Bedrohungen, Netzwerkangriffe und entsprechende Desinfektionsmethoden.
2. Aufgrund der Analyseergebnisse sind folgende Varianten für das Verhalten von Kaspersky Anti-Virus möglich:
 - a. Wenn in der Datei schädlicher Code gefunden wird, sperrt der Datei-Anti-Virus die Datei, erstellt seine Sicherungskopie und versucht, die Desinfektion durchzuführen. Bei erfolgreicher Desinfektion wird die Datei zum Zugriff freigegeben. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht.
 - b. Wenn in der Datei ein Code gefunden wird, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird die Datei der Desinfektion unterzogen und in den Quarantänespeicher verschoben.

- c. Wenn in der Datei kein schädlicher Code gefunden wird, wird sie sofort zum Zugriff freigegeben.

Beim Fund eines infizierten oder möglicherweise infizierten Objekts werden Sie vom Programm darüber informiert. Beim Fund eines infizierten oder möglicherweise infizierten Objekts erscheint auf dem Bildschirm eine Meldung mit einer Anfrage für das weitere Vorgehen. Ihnen wird vorgeschlagen:

- Der Start des Objekts wird auf dem Computer gesperrt oder der Benutzer wird nach den weiteren Aktionen gefragt: Die Bedrohung in die Quarantäne verschieben, um sie später mit Hilfe aktualisierter Datenbanken zu untersuchen und zu bearbeiten.
- Das Objekt löschen.
- Objekt überspringen, wenn Sie absolut sicher sind, dass es unschädlich ist.

SICHERHEITSSTUFE FÜR DATEIEN UND SPEICHER ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Datei-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten. Für die Sicherheitsstufe stehen folgende Varianten zur Auswahl:

- **Hoch.** Wählen Sie diese Stufe, wenn Sie das Infektionsrisiko für Ihren Computer sehr hoch einschätzen.
- **Empfohlen.** Diese Stufe bietet ein ausgewogenes Verhältnis zwischen Leistung und Sicherheit. Sie ist für die meisten Situationen geeignet.
- **Niedrig.** Wenn Sie in einer geschützten Umgebung arbeiten (z.B. in einem Firmennetzwerk mit zentralem Sicherheitssystem), ist die niedrige Sicherheitsstufe geeignet. Die niedrige Sicherheitsstufe kann auch bei der Arbeit mit ressourcenaufwändigen Programmen gewählt werden.

Es wird empfohlen, vor der Auswahl der niedrigen Sicherheitsstufe die vollständige Untersuchung des Computers mit der hohen Sicherheitsstufe vorzunehmen.

Wenn keine vordefinierte Stufe Ihren Anforderungen entspricht, können Sie die Einstellungen (s. Abschnitt "Schutz des Computer-Dateisystems" auf S. 42) von Datei-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

➔ Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Dateien und Speicher zu ändern:

1. Öffnen Sie das Programmfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Datei-Anti-Virus weist gefundenen Objekten aufgrund der Untersuchungsergebnisse einen der folgenden Status zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Wenn Kaspersky Anti-Virus bei einer Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Sie werden dazu aufgefordert, auf die gefundene Bedrohung zu reagieren, indem Sie eine Aktion für das Objekt auswählen. Standardmäßig ist in Kaspersky Anti-Virus als Aktion für ein gefundenes Objekt die Variante **Aktion erfragen** festgelegt. Sie können die Aktion ändern. Wenn Sie beispielsweise sicher sind, dass versucht werden soll, alle gefundenen Objekte zu desinfizieren, und bei einer Meldung über den Fund eines infizierten oder verdächtigen Objekts nicht jedes Mal die Aktion **Desinfizieren** auswählen möchten, dann legen Sie folgende Aktion fest: **Aktion ausführen. Desinfizieren**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 28) arbeiten, wendet Kaspersky Anti-Virus automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige Objekte ist es **Überspringen**.

➡ Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Geben Sie die entsprechende Aktion für die gewählte Komponente an.

SCHUTZBEREICH FESTLEGEN

Unter dem Schutzbereich wird nicht nur der Ort der Untersuchungsobjekte verstanden, sondern auch der Typ der zu untersuchenden Dateien. Kaspersky Anti-Virus untersucht standardmäßig nur potentiell infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden.

Sie können den Schutzbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen / entfernen oder die Typen der zu untersuchenden Dateien ändern. Sie können beispielsweise nur exe-Dateien, die von Netzlaufwerken aus gestartet werden, untersuchen lassen. Allerdings sollten Sie sicherstellen, dass eine Einschränkung des Schutzbereichs nicht zu einem Sicherheitsrisiko für Ihren Computer führt.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. *txt*), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (*exe*, *dll*, *doc*). Das Risiko, dass schädlicher Code in solche Dateien eindringt und später aktiviert wird, ist relativ hoch.
- Ein Angreifer kann einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden, obwohl es sich dabei in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn die Variante  **Dateien nach Erweiterung untersuchen** gewählt wurde, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Variante  **Dateien nach Format untersuchen** gewählt, so ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format *exe* besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

➡ Gehen Sie folgendermaßen vor, um die Liste der Untersuchungsobjekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.

4. Klicken Sie auf der Registerkarte **Allgemein** im Abschnitt **Schutzbereich** auf den Link **Hinzufügen**.
5. Wählen Sie im Fenster **Untersuchungsobjekt auswählen** ein Objekt aus und klicken Sie auf **Hinzufügen**.
6. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie im Fenster **Untersuchungsobjekt auswählen** auf die Schaltfläche **OK**.
7. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

➡ *Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Dateitypen** den gewünschten Parameter.

HEURISTISCHE ANALYSE VERWENDEN

In der Grundeinstellung erfolgt die Untersuchung auf Basis der Datenbanken, die eine Beschreibung der bekannten Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Kaspersky Anti-Virus vergleicht ein gefundenes Objekt mit den Einträgen in den Datenbanken, wodurch sich eindeutig ermitteln lässt, ob das untersuchte Objekt schädlich ist und welcher Malware-Klasse es gegebenenfalls angehört. Dieses Vorgehen wird als *Signaturanalyse* bezeichnet und wird standardmäßig verwendet.

Allerdings tauchen jeden Tag neue schädliche Objekte auf, die noch nicht in die Datenbanken aufgenommen wurden. Bei der Erkennung solcher Objekte hilft die heuristische Analyse. Diese Methode umfasst die Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalysierer von ihrer Aktivität wissen.

Beim Fund eines schädlichen Objekts erhalten Sie eine Meldung mit einer Anfrage für das weitere Vorgehen.

Zusätzlich kann das Genauigkeitsniveau der Untersuchung festgelegt werden. Es reguliert das Verhältnis zwischen Ausführlichkeit der Suche, Auslastungsniveau der Betriebssystemressourcen und Untersuchungsdauer. Je höher das für die Untersuchung gewählte Niveau, desto mehr Systemressourcen sind dafür erforderlich und desto mehr Zeit wird beansprucht.

➡ *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden und die Untersuchungsgenauigkeit festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchungsmethoden** das Kontrollkästchen  **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe ein.

UNTERSUCHUNG OPTIMIEREN

Um die Untersuchungsdauer zu reduzieren und die Arbeitsgeschwindigkeit von Kaspersky Anti-Virus zu steigern, können Sie festlegen, dass nur neue Dateien und Dateien, die seit ihrer letzten Analyse verändert wurden, untersucht werden. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

➡ *Gehen Sie folgendermaßen vor, damit nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchung optimieren** das Kontrollkästchen  **Nur neue und veränderte Dateien untersuchen**.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Installationspakete und Dateien, die OLE-Objekte enthalten, werden beim Öffnen ausgeführt und gelten deshalb als gefährlicher als Archive. Indem die Untersuchung von Archiven deaktiviert und die Untersuchung von Dateien dieser Typen aktiviert wird, schützen Sie Ihren Computer vor der Ausführung von schädlichem Code und senken gleichzeitig die Untersuchungsgeschwindigkeit.

In der Grundeinstellung untersucht Kaspersky Anti-Virus nur angehängte OLE-Objekte.

➡ *Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** die Kontrollkästchen  der zusammengesetzten Dateien, die vom Programm untersucht werden sollen.

UNTERSUCHUNG UMFANGREICHER ZUSAMMENGESETZTER DATEIEN

Bei der Untersuchung von umfangreichen zusammengesetzten Dateien kann das vorausgehende Entpacken viel Zeit beanspruchen. Die Dauer kann reduziert werden, wenn die Untersuchung von Dateien im Hintergrundmodus erfolgt. Wenn bei der Arbeit mit einer solchen Datei ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Anti-Virus darüber informiert.

Um die Verzögerung beim Zugriff auf zusammengesetzte Dateien zu reduzieren, kann das Entpacken von Dateien, die eine bestimmte Größe überschreiten, deaktiviert werden. Beim Extrahieren aus Archiven werden Dateien immer untersucht.

➤ *Gehen Sie folgendermaßen vor, damit Kaspersky Anti-Virus umfangreiche Dateien im Hintergrundmodus entpackt:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☒ **Zusammengesetzte Dateien im Hintergrund entpacken** und legen Sie im Feld unten die minimale Dateigröße fest.

➤ *Gehen Sie folgendermaßen vor, damit Kaspersky Anti-Virus umfangreiche zusammengesetzte Dateien nicht entpackt:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte **Leistung** im Abschnitt **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☒ **Große zusammengesetzte Dateien nicht entpacken** und legen Sie im Feld unten einen Wert für die maximale Dateigröße fest.

UNTERSUCHUNGSMODUS ÄNDERN

Unter Untersuchungsmodus wird die Bedingung für das Auslösen von Datei-Anti-Virus verstanden. In der Grundeinstellung verwendet Kaspersky Anti-Virus den intelligenten Modus, in dem die Entscheidung über die Untersuchung eines Objekts auf Basis der Operationen, die damit ausgeführt werden sollen, gefällt wird. Beispielsweise untersucht Kaspersky Anti-Virus bei der Arbeit mit einem Microsoft Office-Dokument eine Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Sie können den Untersuchungsmodus für Objekte ändern. Der passende Modus ist davon abhängig, mit welcher Art von Dateien Sie überwiegend arbeiten.

➤ *Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie auf der Registerkarte **Erweitert** im Abschnitt **Untersuchungsmodus** den gewünschten Modus.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich können Sie die Technologie auswählen, die Datei-Anti-Virus verwenden soll:

- **iChecker.** Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Objekte ausgeschlossen werden. Objekte werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Anti-Virus, das Datum der letzten Untersuchung des Objekts und Veränderungen der Untersuchungsparameter berücksichtigt.

Es kann beispielsweise sein, dass einer Archivdatei aufgrund der Untersuchungsergebnisse der Status *virenfrei* zugewiesen wurde. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit großen Dateien und kann nur auf Objekte angewandt werden, deren Struktur dem Programm bekannt ist (z.B. die Dateiformate *exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar*).

- **iSwift.** Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

➡ Gehen Sie folgendermaßen vor, um die Untersuchungstechnologie für Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** den erforderlichen Parameterwert.

KOMPONENTE ANHALTEN: ZEITPLAN ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit von Datei-Anti-Virus vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann in den Einstellungen festgelegt werden, dass die Komponente für einen bestimmten Zeitraum angehalten wird.



Abbildung 7. Zeitplan erstellen

➡ Gehen Sie folgendermaßen vor, um den Zeitplan anzupassen, nach dem eine Komponente angehalten werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.

3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** ☒ das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf die Schaltfläche **Zeitplan**.
5. Geben Sie im Fenster **Aufgabe anhalten** in den Feldern **Anhalten um** und **Fortsetzen um** den erforderlichen Zeitraum an (im Format HH:MM).

KOMPONENTE ANHALTEN: LISTE DER PROGRAMME ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit von Datei-Anti-Virus vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann in den Einstellungen festgelegt werden, dass die Komponente bei der Arbeit mit bestimmten Programmen angehalten wird.

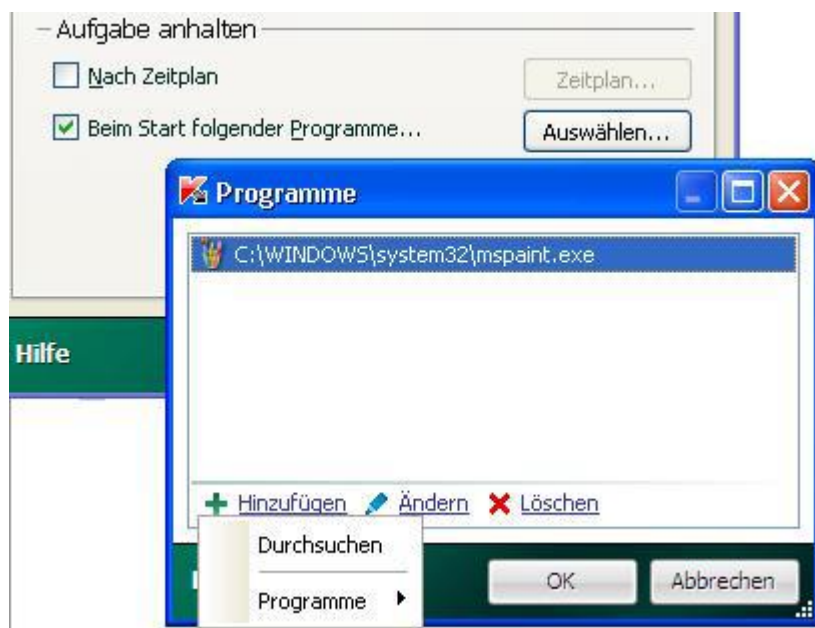


Abbildung 8. Liste der Programme erstellen

Das Deaktivieren von Datei-Anti-Virus bei einem Konflikt mit bestimmten Programmen gilt als Notlösung! Sollten bei der Arbeit der Komponente Konflikte auftreten, dann wenden Sie sich an den technischen Support von Kaspersky Lab (<http://support.kaspersky.de>). Die Spezialisten helfen Ihnen dabei, auf Ihrem Computer die gemeinsame Arbeit von Kaspersky Anti-Virus mit anderen Programmen einzurichten.

- Gehen Sie folgendermaßen vor, um festzulegen, dass die Komponente angehalten wird, während die angegebenen Programme arbeiten:
1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
 2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
 3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
 4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen ☒ **Beim Start folgender Programme** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

STANDARDMÄßIGE SCHUTZPARAMETER WIEDERHERSTELLEN

Während Sie die Arbeit von Datei-Anti-Virus konfigurieren, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

➡ *Gehen Sie folgendermaßen vor, um die standardmäßigen Schutzeinstellungen wiederherzustellen,*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

E-MAIL-SCHUTZ

Mail-Anti-Virus untersucht, ob in ein- und ausgehenden E-Mails gefährliche Objekte vorhanden sind. Mail-Anti-Virus wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mails der Protokolle POP3, SMTP, IMAP, MAPI und NNTP.

Die E-Mail-Untersuchung erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Wenn eine Bedrohung festgestellt wird, führt Mail-Anti-Virus die vorgegebene Aktion (s. Abschnitt "Aktion für gefundene Objekte ändern" auf S. 54) aus. Die Regeln, nach denen die Untersuchung Ihrer Post erfolgt, werden durch eine Anzahl von Parametern bestimmt. Sie lassen sich in Gruppen unterteilen, die folgende Details festlegen:

- geschützter E-Mail-Datenstrom.
- heuristische Analysemethoden verwenden.
- Untersuchung von zusammengesetzten Dateien.
- Filterung angehängter Dateien.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Mail-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine andere Sicherheitsstufe auszuwählen. Sie können die Standardeinstellungen von E-Mail-Anti-Virus wiederherstellen. Wählen Sie dazu eine Sicherheitsstufe aus.

➡ Gehen Sie folgendermaßen vor, um die Funktionsparameter von Mail-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente	53
Sicherheitsstufe für den E-Mail-Schutz ändern	53
Aktion für gefundene Objekte ändern	54
Schutzbereich festlegen	55
E-Mail-Untersuchung in Microsoft Office Outlook	55
E-Mail-Untersuchung in The Bat!	56
Heuristische Analyse verwenden	57
Untersuchung von zusammengesetzten Dateien	57
Anlagenfilterung	57
Standardparameter für den Mail-Schutz wiederherstellen	58

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Mail-Anti-Virus ist eine Komponente von Kaspersky Anti-Virus, die die Untersuchung von E-Mails auf gefährliche Objekte gewährleistet. Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mail-Nachrichten der Protokolle POP3, SMTP, IMAP, MAPI und NNTP, sowie über geschützte Verbindungen (SSL) mit den Protokollen POP3 und IMAP.

Als Indikator für die Arbeit der Komponente dient das Symbol im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer E-Mail das Aussehen  annimmt.

Der E-Mail-Schutz erfolgt standardmäßig nach folgendem Algorithmus:

1. Jede Nachricht, die vom Benutzer empfangen oder gesendet wird, wird von der Komponente abgefangen.
2. Die E-Mail-Nachricht wird in ihre Bestandteile zerlegt: Kopfzeile, Briefkörper, Anhänge.
3. Der Körper und die Anhänge der E-Mail-Nachricht (einschließlich eingebetteten OLE-Objekten) werden auf gefährliche Objekte untersucht. Schädliche Objekte werden auf Basis der Datenbanken erkannt, die bei der Arbeit von Kaspersky Anti-Virus verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.
4. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:
 - Wenn der Körper oder ein Anhang der Nachricht schädlichen Code enthält, sperrt der Schutz für E-Mails und Instant-Messenger die E-Mail, speichert eine Sicherungskopie davon im Backup und versucht das Objekt zu desinfizieren. Bei erfolgreicher Desinfektion erhält der Benutzer Zugriff auf die E-Mail. Wenn die Desinfektion fehlschlägt, wird das infizierte Objekt aus der Nachricht gelöscht. Als Ergebnis der Antiviren-Bearbeitung wird in die Betreffzeile der E-Mail ein spezieller Text eingefügt, der darüber informiert, dass sie von Kaspersky Anti-Virus bearbeitet wurde.
 - Wenn der Körper oder ein Anhang der Nachricht einen Code enthält, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird der verdächtige Teil der Nachricht in die Quarantäne verschoben.
 - Wenn in der E-Mail kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff darauf.

Für das Mailprogramm Microsoft Office Outlook ist ein integrierbares Erweiterungsmodul (s. Abschnitt "E-Mail-Untersuchung in Microsoft Office Outlook" auf S. 55) vorgesehen, mit dem die Untersuchung von E-Mails feiner eingestellt werden kann.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky Anti-Virus zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Verarbeitung des Mailverkehrs (s. Abschnitt "E-Mail-Untersuchung in The Bat!" auf S. 56) direkt in The Bat! eingestellt und haben Vorrang vor den Parametern für den E-Mail durch die Anwendung.

Bei der Arbeit mit anderen Mailprogrammen (einschließlich Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, IncrediMail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails, die mit dem IMAP-Protokoll übertragen werden, nicht auf Viren untersucht werden, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

SICHERHEITSTUFE FÜR DEN E-MAIL-SCHUTZ ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Mail-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der

Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten. Folgende Sicherheitsstufen stehen zur Auswahl:

- **Hoch.** Wenn Sie in einer gefährlichen Umgebung arbeiten, ist die maximale Sicherheitsstufe geeignet. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk erfolgt, das nicht über einen zentralisierten E-Mail-Schutz verfügt.
- **Empfohlen.** Diese Stufe bietet ein ausgewogenes Verhältnis zwischen Leistung und Sicherheit. Sie ist für die meisten Situationen geeignet. Die empfohlene Stufe entspricht der Grundeinstellung.
- **Niedrig.** Wenn Sie in einer gut geschützten Umgebung arbeiten, ist die niedrige Sicherheitsstufe geeignet. Als Beispiel für eine solche Umgebung kann ein Firmennetzwerk mit zentralisiertem E-Mail-Schutz dienen.

Wenn keine vordefinierte Stufe Ihren Anforderungen entspricht, können Sie die Einstellungen (s. Abschnitt "Schutz für E-Mail" auf S. 52) von Mail-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

➡ Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für E-Mails zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Mail-Anti-Virus untersucht E-Mail-Nachrichten. Wenn sich durch die Virenuntersuchung ergibt, dass eine E-Mail oder ein E-Mail-Objekt (Briefkörper, Anhang) infiziert oder möglicherweise infiziert ist, sind die weiteren Operationen, die die Komponente ausführt, vom Status des Objekts und von der ausgewählten Aktion abhängig.

Mail-Anti-Virus weist gefundenen Objekten aufgrund des Untersuchungsergebnisses einen der folgenden Status zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der E-Mail oder in einem E-Mail-Objekt die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Wenn Kaspersky Anti-Virus bei einer E-Mail-Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Sie werden dazu aufgefordert, auf die gefundene Bedrohung zu reagieren, indem Sie eine Aktion für das Objekt auswählen. Standardmäßig ist in Kaspersky Anti-Virus als Aktion für ein gefundenes Objekt die Variante **Aktion erfragen** festgelegt. Sie können die Aktion ändern. Wenn Sie beispielsweise sicher sind, dass versucht werden soll, alle gefundenen Objekte zu desinfizieren, und bei einer Meldung über den Fund eines infizierten oder verdächtigen Objekts in einer E-Mail nicht jedes Mal die Aktion **Desinfizieren** auswählen möchten, dann legen Sie folgende Aktion fest: **Aktion ausführen. Desinfizieren**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 28) arbeiten, wendet Kaspersky Anti-Virus automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich, für verdächtige – Überspringen**.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Geben Sie die entsprechende Aktion für die gewählte Komponente an.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky Anti-Virus sowohl eingehende, als auch ausgehende E-Mails. Wenn Sie nur die Untersuchung eingehender E-Mails gewählt haben, ist es empfehlenswert, zu Beginn der Arbeit mit Kaspersky Anti-Virus die ausgehenden E-Mails zu untersuchen, weil sich auf Ihrem Computer Mailwürmer befinden können, die E-Mails als Kanal verwenden, um sich weiterzuverbreiten. Dadurch wird erlaubt, Probleme zu verhindern, die mit dem unkontrollierten Versenden infizierter E-Mails von Ihrem Computer verbunden sind.

Zum Schutzbereich gehören auch die Parameter für die Integration von Mail-Anti-Virus in das System und die zu untersuchenden Protokolle. In der Grundeinstellung wird Mail-Anti-Virus in die Mailprogramme Microsoft Office Outlook und The Bat! integriert.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender E-Mails auszuschalten:*

1. Öffnen Sie das das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Geben Sie im folgenden Fenster Registerkarte **Allgemein** im Block **Schutzbereich** die gewünschten Parameterwerte an.

➡ *Gehen Sie folgendermaßen vor, um die zu untersuchenden Protokolle und die Parameter für die Integration von Mail-Anti-Virus in das System festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Integration ins System** die erforderlichen Parameter.

E-MAIL-UNTERSUCHUNG IN MICROSOFT OFFICE OUTLOOK

Wenn Microsoft Office Outlook als Mailprogramm verwendet wird, können Sie die Virenuntersuchung Ihrer E-Mails zusätzlich anpassen.

Bei der Installation von Kaspersky Anti-Virus wird ein spezielles Erweiterungsmodul in Microsoft Office Outlook integriert. Es erlaubt Ihnen, schnell zu den Einstellungen von Mail-Anti-Virus zu wechseln und festzulegen, wann eine E-Mail-Nachricht auf das Vorhandensein gefährlicher Objekte untersucht werden soll.

Das Erweiterungsmodul besitzt die Form einer speziellen Registerkarte mit dem Namen **E-Mail-Schutz**, die sich im Menü **Extras** → **Optionen** befindet. Auf der Registerkarte können Sie die Untersuchungsmodi für E-Mail festlegen.

➡ *Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für E-Mails festzulegen:*

1. Öffnen Sie das Hauptfenster von Microsoft Office Outlook.
2. Wählen Sie im Programmmenü den Punkt **Extras** → **Optionen**.
3. Legen Sie auf der Registerkarte **E-Mail-Schutz** den erforderlichen Modus für die E-Mail-Untersuchung fest.

E-MAIL-UNTERSUCHUNG IN THE BAT!

Die Aktionen für infizierte E-Mail-Objekte werden im Mailprogramm The Bat! durch Mittel des Programms festgelegt.

Die Parameter von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende E-Mails untersucht werden, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich die Untersuchung angehängter Archive.

Die hier angezeigten Parameter für den E-Mail-Schutz gelten für alle auf dem Computer installierten Antiviren-Module, die die Arbeit mit The Bat! unterstützen.

Es sollte beachtet werden, dass E-Mails beim Empfang zuerst von Mail-Anti-Virus untersucht werden und erst anschließend von dem Plug-in des Mailprogramms The Bat!. Wenn ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Anti-Virus auf jeden Fall darüber informiert. Wenn dabei im Meldungsfenster von Mail-Anti-Virus die Aktion **Desinfizieren (Löschen)** gewählt wird, führt Mail-Anti-Virus das Löschen der Bedrohung aus. Wird im Meldungsfenster die Aktion **Überspringen** gewählt, so wird das Objekt von dem Plug-in für The Bat! desinfiziert. Beim Senden werden E-Mails zuerst von dem Plug-in und anschließend von Mail-Anti-Virus untersucht.

Folgende Einstellungen sind erforderlich:

- Welche Richtung des E-Mail-Verkehrs (eingehende, ausgehende) der Untersuchung unterzogen werden soll.
- Wann die Untersuchung von E-Mail-Objekten erfolgen soll (beim Öffnen einer E-Mail oder vor dem Speichern auf der Festplatte).
- Aktionen, die das Mailprogramm ausführen soll, wenn gefährliche Objekte in E-Mails gefunden werden. Es stehen beispielsweise zur Auswahl:
 - **Reparaturversuch infizierter Teile** – Bei Auswahl dieser Variante wird versucht, ein infiziertes Objekt zu desinfizieren. Wenn die Desinfektion fehlschlägt, verbleibt das Objekt in der Nachricht.
 - **Infizierte Teile löschen** – Bei Auswahl dieser Variante wird ein gefährliches E-Mail-Objekt gelöscht. Dabei bleibt unberücksichtigt, ob es infiziert ist oder als verdächtig gilt.

Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in die Quarantäne.

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden von dem Programm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

➡ *Gehen Sie folgendermaßen vor, um in The Bat! die Einstellungen für den E-Mail-Schutz anzupassen:*

1. Öffnen Sie das Hauptfenster von The Bat!.
2. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
3. Wählen Sie in der Konfigurationsstruktur den Punkt **Anti-Virus-Plug-Ins**.

HEURISTISCHE ANALYSE VERWENDEN

Die heuristische Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Kaspersky Anti-Virus informiert Sie darüber, wenn in einer Nachricht ein schädliches Objekt gefunden wird. Die Meldung erfordert die Auswahl einer Aktion.

Zusätzlich können Sie das Genauigkeitsniveau der Untersuchung festlegen: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

➡ *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden / zu deaktivieren und die Genauigkeitsstufe der Untersuchung festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Untersuchungsmethoden** das Kontrollkästchen ☒ **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau ein.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Die Auswahl des Untersuchungsmodus für zusammengesetzte Dateien beeinflusst die Leistung von Kaspersky Anti-Virus. Sie können die Untersuchung angehängter Archive aktivieren oder deaktivieren, sowie die maximale Größe der zu untersuchenden Archive begrenzen.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchungsparameter für zusammengesetzte Dateien anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** den Untersuchungsmodus für zusammengesetzte Dateien.

ANLAGENFILTERUNG

Sie können die Filterbedingungen für an E-Mails angehängte Objekte anpassen. Die Verwendung des Filters bietet Ihrem Computer zusätzliche Sicherheit, da sich in E-Mails enthaltene Malware meist in angehängten Dateien befindet. Das Umbenennen oder Löschen von Attachments eines bestimmten Typs erlaubt es, Ihren Computer beispielsweise davor zu schützen, dass eine angehängte Datei beim Empfang einer Nachricht automatisch geöffnet wird.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist (die Internetverbindung erfolgt ohne Proxyserver oder Firewall), wird davor gewarnt, die Untersuchung angehängter Archive zu deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um die Parameter für die Anlagenfilterung anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Legen Sie im folgenden Fenster auf der Registerkarte **Anlagenfilterung** die Bedingungen für die Filterung von Objekten fest, die an E-Mails angehängt sind. Bei Auswahl der letzten beiden Modi wird die Liste der Dateitypen aktiviert. In dieser Liste können Sie die erforderlichen Typen ankreuzen oder die Maske eines neuen Typs hinzufügen.

Wenn ein neuer Maskentyp hinzugefügt werden soll, klicken Sie auf den Link **Hinzufügen** und geben Sie im folgenden Fenster **Maske für Dateinamen** die erforderlichen Daten ein.

STANDARDPARAMETER FÜR DEN MAIL-SCHUTZ WIEDERHERSTELLEN

Während Sie die Arbeit von Mail-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

➡ *Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Mail-Schutz wiederherzustellen,*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

SCHUTZ FÜR WEB-DATENVERKEHR

Immer wenn Sie im Internet arbeiten, besteht für die Informationen, die auf Ihrem Computer gespeichert sind, das Risiko einer Infektion durch gefährliche Programme. Sie können in Ihren Computer eindringen, während Sie kostenlose Programme herunterladen oder scheinbar ungefährliche Seiten besuchen (die zuvor von Hackern angegriffen wurden). Außerdem können Netzwürmer direkt beim Aufbau einer Internetverbindung in Ihren Computer eindringen, bevor überhaupt eine Webseite geöffnet oder eine Datei heruntergeladen wird.

Die Sicherheit Ihrer Arbeit im Internet wird von der Komponente *Web-Anti-Virus* gewährleistet. Er schützt Informationen, die über das HTTP-Protokoll auf Ihren Computer gelangen, und verhindert den Start gefährlicher Skripts auf Ihrem Computer.

Der Web-Schutz sieht nur die Kontrolle des HTTP-Datenverkehrs vor, der über die Ports, die in der Liste zu kontrollierenden Ports angegeben sind, übertragen wird. Eine Liste der Ports, die am häufigsten zur Übertragung von E-Mails und HTTP-Datenverkehr benutzt werden, ist im Lieferumfang von Kaspersky Anti-Virus enthalten. Wenn Sie Ports verwenden, die nicht zu dieser Liste gehören, sollten diese der Liste hinzugefügt werden, um den Schutz des über sie abgewickelten Datenverkehrs zu gewährleisten.

Wenn Sie in einer ungeschützten Umgebung arbeiten, ist es empfehlenswert, bei der Arbeit im Internet die Komponente Web-Anti-Virus zu verwenden. Wenn Ihr Computer in einem Netzwerk arbeitet, das durch eine Firewall oder durch HTTP-Traffic-Filter gesichert ist, gewährleistet Web-Anti-Virus dem Computer zusätzliche Sicherheit.

Die Untersuchung des Datenverkehrs erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Beim Fund von Bedrohungen führt Web-Anti-Virus die festgelegte Aktion aus.

Das Schutzniveau, das auf Ihrem Computer für den Web-Datenverkehr gilt, wird durch eine Auswahl von Parametern festgelegt. Sie lassen sich in folgende Gruppen aufteilen:

- Parameter, die den Schutzbereich definieren.
- Parameter, die die Leistung des Schutzes für den Datenverkehr (Heuristische Analyse verwenden, Untersuchung optimieren) festlegen.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Web-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine andere Sicherheitsstufe auszuwählen.

➡ Gehen Sie folgendermaßen vor, um die Funktionsparameter von Web-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Passen Sie die Parameter der Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente	60
Sicherheitsstufe für den HTTP-Datenverkehr ändern	61
Aktion für gefundene Objekte ändern	61
Schutzbereich festlegen	62
Untersuchungstyp auswählen	62
Modul zur Link-Untersuchung	63
Heuristische Analyse verwenden	64
Untersuchung optimieren	64
Standardparameter für den Web-Schutz wiederherstellen	65

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Web-Anti-Virus schützt Informationen, die über das HTTP-Protokoll auf Ihren Computer gelangen, und verhindert auf Ihrem Computer den Start gefährlicher Skripts.

Im Folgenden wird das Funktionsschema der Komponente näher beschrieben. Der Schutz des HTTP-Verkehrs erfolgt nach folgendem Algorithmus:

1. Jede Webseite oder Datei, auf die ein Benutzer oder ein bestimmtes Programm über das HTTP-Protokoll zugreift, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert. Die Suche nach schädlichen Objekten erfolgt auf Basis der Datenbanken, die bei der Arbeit von Kaspersky Anti-Virus verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.
2. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:
 - Wenn eine Webseite oder ein Objekt, auf das ein Benutzer zugreift, schädlichen Code enthält, wird der Zugriff darauf blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass das angeforderte Objekt oder die Seite infiziert ist.
 - Wenn die Datei oder Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf.

Die Untersuchung von Skripts wird nach folgendem Algorithmus ausgeführt:

1. Jedes auf einer Webseite auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.
2. Wenn ein Skript schädlichen Code enthält, wird es von Web-Anti-Virus gesperrt und der Benutzer wird durch eine spezielle Popupmeldung benachrichtigt.
3. Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

Skripts werden nur auf Webseiten abgefangen, die mit Microsoft Internet Explorer gestartet werden.

SICHERHEITSTUFE FÜR DEN HTTP-DATENVERKEHR

ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Web-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten. Für die Sicherheitsstufe stehen folgende Varianten zur Auswahl:

- **Hoch.** Es wird empfohlen, diese Stufe in einer aggressiven Umgebung zu verwenden, wenn keine anderen Mittel zum Schutz des HTTP-Datenverkehrs eingesetzt werden.
- **Empfohlen.** Diese Sicherheitsstufe gilt für die meisten Situationen als optimal.
- **Niedrig.** Verwenden Sie diese Sicherheitsstufe, wenn auf Ihrem Computer zusätzliche Mittel zum Schutz des HTTP-Datenverkehrs installiert sind.

Wenn keine vordefinierte Stufe Ihren Anforderungen entspricht, können Sie die Einstellungen (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. [59](#)) von Web-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für den Web-Datenverkehr zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Legen Sie die erforderliche Sicherheitsstufe für die gewählte Komponente fest.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Wenn sich bei der Analyse eines Objekts des HTTP-Verkehrs herausstellt, dass das Objekt schädlichen Code enthält, sind die weiteren Operationen, die Web-Anti-Virus ausführt, von der Aktion abhängig, die Sie festgelegt haben.

Was die Aktionen für gefährliche Skripts betrifft, so sperrt Web-Anti-Virus deren Ausführung immer und zeigt auf dem Bildschirm eine Popupmeldung an, die den Benutzer über die ausgeführte Aktion informiert. Die Aktion für das gefährliche Objekt kann nicht geändert werden, es kann nur das Modul für die Skript-Untersuchung ausgeschaltet werden (s. Abschnitt "Untersuchungstyp auswählen" auf S. [62](#)).

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. [28](#)) arbeiten, wendet Kaspersky Anti-Virus automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:*

1. Öffnen Sie Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Geben Sie die entsprechende Aktion für die gewählte Komponente an.

SCHUTZBEREICH FESTLEGEN

Das Festlegen des Schutzbereichs umfasst die Auswahl des von Web-Anti-Virus verwendeten Untersuchungstyps für Objekte (s. Abschnitt "Untersuchungstyp auswählen" auf S. 62) und das Anlegen einer Liste mit vertrauenswürdigen Webadressen, deren Informationen von der Komponente nicht auf Viren analysiert werden sollen.

Sie können eine Liste der vertrauenswürdigen Webadressen anlegen, deren Inhalt Sie vorbehaltlos vertrauen. Web-Anti-Virus wird die Informationen von diesen Adressen nicht auf gefährliche Objekte hin analysieren. Diese Option kann benutzt werden, wenn Web-Anti-Virus das Laden einer bestimmten Datei verhindert, indem er den Downloadversuch blockiert.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchung optimieren** das Kontrollkästchen ☒ **HTTP-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** und klicken Sie auf die Schaltfläche **Auswählen**.
5. Klicken Sie im folgenden Fenster **Liste der vertrauenswürdigen Webadressen** auf den Link **Hinzufügen**.
6. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine vertrauenswürdige Adresse (oder ihre Maske) ein.

UNTERSUCHUNGSTYP AUSWÄHLEN

Die Aufgabe Schutzbereich festlegen (s. S. 62) umfasst neben dem Anlegen einer Liste der vertrauenswürdigen Webadressen auch die Auswahl des von Web-Anti-Virus für den Datenverkehr verwendeten Untersuchungstyps. Es wird unterschieden zwischen der Untersuchung von Skripts und der Untersuchung des HTTP-Datenverkehrs.

In der Grundeinstellung führt Web-Anti-Virus gleichzeitig die Untersuchung von HTTP-Datenverkehr und Skripts aus.

Zur Untersuchung des HTTP-Datenverkehrs gehört nicht nur die Untersuchung auf Viren, sondern auch die Untersuchung von Links auf deren Zugehörigkeit zur Liste der verdächtigen Webadressen und / oder zur Liste der Phishing-Webadressen.

Durch die Untersuchung von Links auf die Zugehörigkeit zur Liste der Phishing-Adressen lassen sich Phishing-Angriffe abwehren, die in der Regel die Form von E-Mails besitzen, die scheinbar von finanziellen Institutionen stammen und Links auf deren Webseiten enthalten. Die Nachricht fordert dazu auf, einem Link zu folgen und auf der betreffenden Seite vertrauliche Informationen wie beispielsweise eine Kreditkartennummer oder Benutzername und Kennwort für die persönliche Internet-Banking-Seite einzugeben, auf der finanzielle Operationen erfolgen können.

Da Links, die auf Phishing-Seiten verweisen, nicht nur mit E-Mails, sondern auch mit anderen Mitteln (beispielsweise im Text einer ICQ-Nachricht) an Sie geschickt werden können, überwacht und blockiert die Komponente Web-Anti-Virus alle Versuche zum Öffnen einer Phishing-Seite auf der Ebene des HTTP-Datenverkehrs.

Die Untersuchung von Links auf ihre Zugehörigkeit zur Liste der verdächtigen Webadressen bietet die Kontrolle über Webseiten, die auf der schwarzen Liste stehen. Die Liste wird von den Kaspersky-Lab-Fachleuten angelegt und gehört zum Lieferumfang des Programms.

➡ *Gehen Sie folgendermaßen vor, damit Web-Anti-Virus Skripts untersucht:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Vergewissern Sie sich im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert**, dass das Kontrollkästchen ☒ **Gefährliche Skripts in Microsoft Internet Explorer blockieren** aktiviert ist. In diesem Fall wird Web-Anti-Virus alle Skripts, die in Microsoft Internet Explorer verarbeitet werden, und alle WSH-Skripts (JavaScript, Visual Basic Script u.a.), die bei der Arbeit eines Benutzers auf dem Computer gestartet werden, untersuchen.

Außerdem können Sie das Modul Link-Untersuchung verwenden (s. S. 63). Dazu aktivieren Sie das Kontrollkästchen ☒ **Phishing-Links und verdächtige Links im Microsoft Internet Explorer und Mozilla Firefox kennzeichnen**. Web-Anti-Virus markiert gefundene Phishing-Links und verdächtige Links in den Webadressen der Browser (Microsoft Internet Explorer und Mozilla Firefox).

➡ *Gehen Sie folgendermaßen vor, um Links mit der Datenbank für verdächtige Webadressen und / oder Phishing-Webadressen zu untersuchen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Vergewissern Sie sich, dass im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchungsmethoden** das Kontrollkästchen ☒ **Links mit der Datenbank für verdächtige Webadressen** untersuchen und / oder das Kontrollkästchen ☒ **Links mit der Datenbank für Phishing-Webadressen untersuchen** aktiviert ist.

MODUL ZUR LINK-UNTERSUCHUNG

Kaspersky Anti-Virus umfasst ein Modul zur Link-Untersuchung, das zu der Komponente Web-Anti-Virus gehört. Das Modul untersucht alle Links, die auf einer Webseite vorhanden sind, auf Zugehörigkeit zu verdächtigen und Phishing-Webadressen. Sie können folgende Listen anlegen: eine Liste mit vertrauenswürdigen Adressen von Webseiten, deren Inhalt nicht untersucht werden soll, und eine Liste mit Adressen von Webseiten, deren Inhalt untersucht werden soll. Das Modul wird als Plug-in in die Webbrowser Microsoft Internet Explorer und Mozilla Firefox integriert.

➡ *Gehen Sie folgendermaßen vor, um das Modul zur Link-Untersuchung zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Im folgenden Fenster **Web-Anti-Virus** aktivieren Sie im Block **Erweitert** das Kontrollkästchen ☒ **Phishing-Links und verdächtige Links im Microsoft Internet Explorer und Mozilla Firefox kennzeichnen**.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** auf die Schaltfläche **Einstellungen**.
5. Wählen Sie im folgenden Fenster **Modul zur Link-Untersuchung** die Variante ☒ **Für alle Webadressen** aus und klicken Sie auf die Schaltfläche **Ausnahmen**.

6. Klicken Sie im folgenden Fenster **Liste der vertrauenswürdigen Webadressen** auf den Link Hinzufügen.
7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine vertrauenswürdige Adresse (oder ihre Maske) ein.

➡ *Gehen Sie folgendermaßen vor, um eine Liste der Webadressen von Seiten anzulegen, deren Inhalt untersucht werden soll:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link Einstellungen.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** auf die Schaltfläche **Einstellungen**.
5. Im folgenden Fenster **Modul zur Link-Untersuchung** wählen Sie auf die Variante  **Für die angegebenen Webadressen** aus und klicken Sie auf die Schaltfläche **Auswählen**.
6. Klicken Sie im folgenden Fenster **Liste der zu untersuchenden Webadressen** auf den Link Hinzufügen.
7. Geben Sie im folgenden Fenster **Adressenmaske (URL)** eine Adresse (oder eine Maske) an.

HEURISTISCHE ANALYSE VERWENDEN

Die heuristische Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalysen von ihrer Aktivität wissen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Kaspersky Anti-Virus informiert Sie darüber, wenn in einer Nachricht ein schädliches Objekt gefunden wird. Die Meldung erfordert die Auswahl einer Aktion.

Zusätzlich kann die Genauigkeitsstufe der Untersuchung festgelegt werden: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

➡ *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden / zu deaktivieren und die Genauigkeitsstufe der Untersuchung festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link Einstellungen.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchungsmethoden** das Kontrollkästchen  **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau der Untersuchung ein.

UNTERSUCHUNG OPTIMIEREN

Um die Erkennungsgenauigkeit für schädlichen Code durch Web-Anti-Virus zu steigern, wird für Objekte, die aus dem Internet eintreffen, die Zwischenspeicherung von Fragmenten verwendet. Bei Verwendung dieser Methode erfolgt die Untersuchung eines Objekts durch Web-Anti-Virus erst, nachdem es vollständig empfangen wurde. Anschließend wird das Objekt auf Viren analysiert und entsprechend der Analyseergebnisse dem Benutzer zur Arbeit übergeben oder blockiert.

Allerdings erhöht die Verwendung dieses Algorithmus die Zeit für die Objektuntersuchung und für dessen Freigabe an den Benutzer. Außerdem können beim Kopieren und bei der Bearbeitung großer Objekte Probleme auftreten, die mit einer Zeitüberschreitung bei der Verbindung mit dem HTTP-Client zusammenhängen.

Um dieses Problem zu lösen, empfehlen wir, die Zeit für die Zwischenspeicherung von Fragmenten eines aus dem Internet empfangenden Objekts zu beschränken. Bei einer Überschreitung der festgelegten Dauer wird jeder heruntergeladene Teil der Dateien ungeprüft dem Benutzer übergeben. Nach dem Abschluss des Downloads wird das Objekt vollständig untersucht. Dadurch lässt sich die Übertragungsdauer des Objekts an den Benutzer verkürzen und das Problem einer Verbindungstrennung lösen, wobei das Sicherheitsniveau bei der Arbeit im Internet nicht gesenkt wird.

Außerdem beträgt das Zeitlimit für die Zwischenspeicherung von Dateifragmenten 1 Sekunde. Wird dieser Wert erhöht oder die Zeitbeschränkung für die Zwischenspeicherung ganz aufgehoben, so wird das Niveau der Antiviren-Untersuchung gesteigert, wobei es aber gleichzeitig zu einer gewissen Verzögerung beim Objektzugriff kommt.

➤ *Gehen Sie folgendermaßen vor, um ein Zeitlimit für die Zwischenspeicherung von Fragmenten festzulegen oder diese Beschränkung aufzuheben:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Aktivieren / deaktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchung optimieren** das Kontrollkästchen ☒ **Zwischenspeicherung von Fragmenten maximal** und geben Sie rechts im Feld den Zeitraum (in Sekunden) an.

STANDARDPARAMETER FÜR DEN WEB-SCHUTZ WIEDERHERSTELLEN

Während Sie die Arbeit von Web-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

➤ *Gehen Sie folgendermaßen vor, um die standardmäßigen Parameter für Web-Anti-Virus wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Klicken Sie für die ausgewählte Komponente im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

SCHUTZ FÜR DEN DATENVERKEHR VON INSTANT-MESSENGERN

In letzter Zeit gewinnen *Instant-Messenger*, die dem Austausch von Sofortnachrichten dienen, immer größere Popularität. Allerdings bringen sie neben nützlichen Funktionen für die Arbeit im Internet auch eine potentielle Bedrohung für die Computersicherheit mit sich. Mit Hilfe von Instant-Messengern können auch Nachrichten übertragen werden, die Links auf Seiten enthalten, die verdächtig sind oder die von Angreifern für Phishing-Angriffe verwendet werden. Schädliche Programme verwenden Instant-Messenger zum Senden von Spam-Nachrichten. Außerdem können Sofortnachrichten Links zu Programmen (oder sogar Programme) enthalten, die Nummern und Kennwörter der Benutzer stehlen.

Die Komponente *IM-Anti-Virus* dient dazu, die Sicherheit der Arbeit mit Instant-Messengern zu gewährleisten. Sie schützt die Informationen, die über Instant-Messenger-Protokolle auf Ihren Computer gelangen.

Das Produkt gewährleistet Sicherheit bei der Arbeit mit einer Vielzahl von Programmen, die dem Sofortaustausch von Nachrichten dienen. Dazu zählen ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru.Agent und IRC.

Die Programme Yahoo! Messenger und Google Talk arbeiten mit dem SSL-Protokoll. Damit IM-Anti-Virus den Datenverkehr dieser Programme untersucht, ist es erforderlich, die Untersuchung geschützter Verbindungen zu verwenden (s. S. [109](#)). Aktivieren Sie dazu im Abschnitt **Netzwerk** das Kontrollkästchen  **Geschützte Verbindungen untersuchen**.

Die Untersuchung des Datenverkehrs erfolgt mit einer bestimmten Auswahl von Parametern. Wenn IM-Anti-Virus in einer Nachricht eine Bedrohung findet, wird die Nachricht durch eine Warnung für den Benutzer ersetzt.

Das Schutzniveau, das auf Ihrem Computer für den Datenverkehr von Instant-Messengern gilt, wird durch eine Auswahl von Parametern festgelegt. Sie lassen sich in folgende Gruppen aufteilen:

- Parameter, die den Schutzbereich festlegen.
- Parameter, die die Untersuchungsmethoden festlegen.

➡ *Gehen Sie folgendermaßen vor, um die Funktionsparameter von IM-Anti-Virus anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Passen Sie die Parameter der ausgewählten Komponente entsprechend an.

IN DIESEM ABSCHNITT

Algorithmus für die Arbeit der Komponente	67
Schutzbereich festlegen	67
Untersuchungsmethode auswählen	67
Heuristische Analyse verwenden	68

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

IM-Anti-Virus ist eine Komponente von Kaspersky Anti-Virus, die die Untersuchung von Nachrichten, die mit Instant-Messengern übertragen werden, auf gefährliche Objekte gewährleistet. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle eingehenden und ausgehenden Nachrichten.

Der Datenverkehr von Instant-Messengern erfolgt standardmäßig nach folgendem Algorithmus:

1. Jede Nachricht, die vom Benutzer empfangen oder gesendet wird, wird von der Komponente abgefangen.
2. IM-Anti-Virus prüft, ob Sofortnachrichten gefährliche Objekte oder Links enthalten, die in den Datenbanken für verdächtige Webadressen und/oder Phishing-Webadressen verzeichnet sind. Wenn eine Bedrohung gefunden wird, wird der Nachrichtentext durch eine Warnung für den Benutzer ersetzt.
3. Wenn in der Nachricht kein Sicherheitsrisiko gefunden wird, erhält der Benutzer Zugriff darauf.

Die von Instant-Messengern übertragenen Dateien untersucht die Komponente Datei-Anti-Virus (s. Abschnitt "Schutz für das Dateisystems des Computers" auf S. 42) beim Speicherversuch.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen.

-  **Eingehende und ausgehende Nachrichten.** Standardmäßig untersucht der IM-Anti-Virus ein- und ausgehende Nachrichten.
-  **Nur eingehende Nachrichten.** Wählen Sie diesen Parameter, wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten. IM-Anti-Virus untersucht nur eingehende Nachrichten.

Kaspersky Anti-Virus untersucht standardmäßig ein- und ausgehende Nachrichten von Instant-Messengern.

Wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten, können Sie die Untersuchung des ausgehenden Datenverkehrs deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender Nachrichten zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Wählen Sie für die ausgewählte Komponente im Block **Schutzbereich** die Variante  **Nur eingehende Nachrichten**.

UNTERSUCHUNGSMETHODE AUSWÄHLEN

Die Untersuchungsmethoden beziehen sich hier auf die Untersuchung der in Instant-Messenger-Nachrichten enthaltenen Links auf ihre Zugehörigkeit zur Liste für verdächtige Adressen und / oder zur Liste der Phishing-Adressen.

-  **Links mit der Datenbank für verdächtige Webadressen untersuchen.** IM-Anti-Virus prüft, ob die in den Nachrichten enthaltenen Links sich auf der schwarzen Liste befinden.
-  **Links mit der Datenbank für Phishing-Webadressen untersuchen.** Die Datenbanken von Kaspersky Anti-Virus enthalten Informationen über die gegenwärtig bekannten Seiten, die für Phishing-Angriffe benutzt werden.

Die Datenbanken werden von den Kaspersky-Lab-Spezialisten durch Adressen erweitert, die von der internationalen Organisation zum Kampf gegen Phishing (The Anti-Phishing Working Group) zur Verfügung gestellt werden. Diese Liste wird beim Update der Datenbanken von Kaspersky Anti-Virus aktualisiert.

➡ *Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Untersuchungsmethoden** das Kontrollkästchen ☒ **Links mit Datenbank für verdächtige Webadressen untersuchen**.

➡ *Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Untersuchungsmethoden** das Kontrollkästchen ☒ **Links mit Datenbank für Phishing-Webadressen untersuchen**.

HEURISTISCHE ANALYSE VERWENDEN

Die heuristische Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Zu diesem Zweck werden alle Skripts, die in Instant-Messenger-Nachrichten enthalten sind, in einer geschützten Umgebung ausgeführt. Wenn die erkannte Aktivität eines Skripts als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Kaspersky Anti-Virus informiert Sie darüber, wenn in einer Nachricht ein schädliches Objekt gefunden wird.

Zusätzlich können Sie das Genauigkeitsniveau der Untersuchung festlegen: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

➡ *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden / zu deaktivieren und die Genauigkeitsstufe der Untersuchung festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Aktivieren / deaktivieren Sie für die ausgewählte Komponente im Block **Untersuchungsmethoden** das Kontrollkästchen ☒ **Heuristische Analyse** stellen Sie darunter das Genauigkeitsniveau ein.

PROAKTIVER SCHUTZ

Kaspersky Anti-Virus schützt nicht nur vor bekannten, sondern auch vor neuen Bedrohungen, über die keine Informationen in den Datenbanken von Kaspersky Anti-Virus vorhanden sind. Diese Möglichkeit wird durch die speziell entwickelten Komponente *Proaktiver Schutz* gewährleistet.

Die präventiven Technologien, auf denen der Proaktive Schutz beruht, erlauben es, einen Zeitverlust zu vermeiden und eine neue Bedrohung zu neutralisieren, bevor sie auf Ihrem Computer Schaden verursachen kann. Im Unterschied zu den reaktiven Technologien, bei denen die Analyse auf Basis von Einträgen der Datenbanken von Kaspersky Anti-Virus erfolgt, identifizieren die Präventivtechnologien eine neue Bedrohung auf Ihrem Computer nach den Aktionsfolgen, die von einem bestimmten Programm ausgeführt werden. Wenn aufgrund der Aktivitätsanalyse die Aktionsfolge eines Programms als verdächtig eingestuft wird, sperrt Kaspersky Anti-Virus seine Aktivität.

➡ Gehen Sie folgendermaßen vor, um die Funktionsparameter des Proaktiven Schutzes zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Passen Sie die Parameter der ausgewählten Komponente entsprechend an.

IN DIESEM ABSCHNITT

Liste der gefährlichen Aktivität verwenden	69
Kontrollregel für gefährliche Aktivität ändern	70
Gruppe mit vertrauenswürdigen Programmen erstellen	71
Kontrolle über Systembenutzerkonten.....	71

LISTE DER GEFÄHRLICHEN AKTIVITÄT VERWENDEN

Beachten Sie, dass die Einstellungen für die Aktivitätskontrolle in Kaspersky Anti-Virus unterschiedlich sind, je nachdem, ob die Anwendung auf einem Computer mit einem der Betriebssysteme Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 oder Microsoft Windows 7 x64 installiert ist als auf einem Computer mit einem anderen Betriebssystem.

Besonderheiten der Einstellungen für die Aktivitätskontrolle für Programme unter dem Betriebssystem Microsoft Windows XP

Die Aktivität der Anwendungen auf Ihrem Computer wird von Kaspersky Anti-Virus kontrolliert. Der Proaktive Schutz reagiert auf eine bestimmte Folge von Programmaktionen. Werden beispielsweise Aktionen erkannt, bei denen sich ein bestimmtes Programm auf eine Netzwerkressource, in den Autostart-Ordner oder in die Systemregistrierung kopiert, und anschließend seine Kopien versendet, so handelt es sich mit hoher Wahrscheinlichkeit um einen Wurm. Als gefährliche Aktionsfolgen zählen außerdem:

- Aktionen, die für trojanische Programme charakteristisch sind.
- Versuche zum Abfangen von Tastatureingaben.
- Versteckte Installation von Treibern.
- Versuche zum Ändern des Betriebssystemkerns.

- Versuche zum Erstellen versteckter Objekte und Prozesse mit negativem PID-Wert.
- Veränderung der HOSTS-Datei.
- Versuche zum Eindringen in andere Prozesse.
- Auftreten von Prozessen, die die Eingabe / Ausgabe von Daten umleiten.
- Versuche zum Senden von DNS-Anfragen.

Die Liste der gefährlichen Aktivitäten wird beim Update von Kaspersky Anti-Virus automatisch ergänzt und kann nicht verändert werden. Allerdings können Sie die Kontrolle bestimmter Typen gefährlicher Aktivität deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um die Kontrolle bestimmter Typen gefährlicher Aktivität zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Deaktivieren Sie im folgenden Fenster **Proaktiver Schutz** das Kontrollkästchen ☒ neben dem Namen der Aktivität, die nicht kontrolliert werden soll.

Besonderheiten der Einstellungen für die Aktivitätskontrolle für Programme unter den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 oder Microsoft Windows 7 x64.

Wenn der Computer unter einem der oben genannten Betriebssysteme läuft, werden nicht alle Ereignisse kontrolliert. Dies hängt mit Besonderheiten dieser Betriebssysteme zusammen. Beispielsweise werden folgende Arten von Ereignissen nicht kontrolliert: *Eindringen in anderen Prozess, Senden von Daten über vertrauenswürdige Programme, Verdächtige Aktivität im System, Zugriff auf geschützten Speicher.*

KONTROLLREGEL FÜR GEFÄHRLICHE AKTIVITÄT ÄNDERN

Die Liste der gefährlichen Aktivitäten wird beim Update von Kaspersky Anti-Virus automatisch ergänzt und kann nicht verändert werden. Sie können:

- die Kontrolle bestimmter Typen Aktivität deaktivieren.
- eine Regel ändern, nach welcher der Proaktive Schutz beim Fund einer gefährlichen Aktivität vorgeht.
- Liste von Ausnahmen (s. S. [106](#)) erstellen, indem Sie die Anwendungen festlegen, deren Aktivität Sie nicht für gefährlich halten.

➡ *Gehen Sie folgendermaßen vor, um eine Regel zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Klicken Sie für die ausgewählte Komponente auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster **Proaktiver Schutz** im Block **Ereignis** das Ereignis aus, für das die Regel geändert werden soll.
5. Legen Sie für das ausgewählte Ereignis mit Hilfe der Links im Block mit der Regelbeschreibung die entsprechenden Parameter fest:

- Klicken Sie auf den Link mit der geltenden Aktion und wählen Sie im folgenden Fenster **Aktion auswählen** die entsprechende Aktion aus.
- Klicken Sie auf den Link für das geltende Intervall (Es wird nicht für alle Aktivitätsarten ein Intervall angegeben) und legen Sie im folgenden Fenster **Versteckte Prozesse erkennen** ein Intervall fest, mit dem die Suche nach versteckten Prozessen ausgeführt werden soll.
- Klicken Sie auf den Link Ein / Aus, um festzulegen, ob ein Bericht über die ausgeführte Operation erstellt werden soll.

GRUPPE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Es besteht die Möglichkeit, eine Liste mit vertrauenswürdigen Programmen anzulegen, deren Aktivität nicht vom Proaktiven Schutz überwacht werden soll. Programme, die eine digitale Signatur besitzen oder in der Datenbank von Kaspersky Security Network enthalten sind, können als vertrauenswürdig eingestuft werden.

➡ *Gehen Sie folgendermaßen vor, damit der Proaktive Schutz Programme, die eine digitale Signatur besitzen und / oder in der Datenbank von Kaspersky Security Network enthalten sind, als vertrauenswürdig betrachtet und nicht über ihre Aktivität informiert:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link Einstellungen.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Vertrauenswürdige Programme** das Kontrollkästchen ☒ **Mit digitaler Signatur** und / oder das Kontrollkästchen ☒ **Die in der Datenbank von Kaspersky Security Network enthalten sind**.

KONTROLLE ÜBER SYSTEMBENUTZERKONTEN

Benutzerkonten regulieren den Zugriff auf das System und definieren den Benutzer und seine Arbeitsumgebung. Dadurch werden Beschädigungen des Betriebssystems oder der Daten anderer Benutzer verhindert. Systemprozesse sind Prozesse, die vom Systembenutzerkonto gestartet wurden.

➡ *Gehen Sie folgendermaßen vor, damit Kaspersky Anti-Virus nicht nur Benutzerprozesse, sondern auch die Aktivität von Systemprozessen überwacht:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link Einstellungen im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Aktivieren Sie für die ausgewählte Komponente im Block **Erweitert** das Kontrollkästchen ☒ **Systembenutzerkonten kontrollieren**.

UNTERSUCHUNG DES COMPUTERS

Die Untersuchung des Computers auf Viren und Schwachstellen ist eine der wichtigsten Funktionen für die Sicherheit des Rechners. Durch die Virensuche lässt sich die Ausbreitung von schädlichem Code erkennen, der aus bestimmten Gründen nicht vom Malware-Schutz erkannt wurde. Durch die Schwachstellen-Suche wird in Programmen das Vorhandensein von Sicherheitslücken erkannt, die Angreifern zur Verbreitung schädlicher Objekte und zum Zugriff auf persönliche Daten dienen können.

Die Fachleute von Kaspersky Lab haben die Aufgaben Virenuntersuchung (s. S. [72](#)) entwickelt, darunter die Untersuchung von Wechseldatenträgern (s. S. [78](#)) sowie die Aufgabe Suche nach Schwachstellen im System und in Programmen (s. S. [82](#)).

➡ Gehen Sie folgendermaßen vor, um die Parameter einer bestimmten Untersuchungsaufgabe zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Virensuche** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**, **Suche nach Schwachstellen**).
3. Nehmen Sie für die ausgewählte Aufgabe die erforderlichen Änderungen vor.

IN DIESEM ABSCHNITT

Virensuche	72
Suche nach Schwachstellen.....	82

VIRENSUCHE

Die Spezialisten von Kaspersky Lab haben folgende Aufgaben für die Virenuntersuchung Ihres Computers vordefiniert.

- **Objekte untersuchen.** Es werden die vom Benutzer festgelegten Objekte untersucht. Es kann ein beliebiges Objekt des Dateisystems auf dem Computer untersucht werden. Im Rahmen dieser Aufgabe können Sie die Parameter anpassen, die für die Untersuchung von Wechseldatenträgern gelten.
- **Vollständige Untersuchung.** Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Schnelle Untersuchung.** Es werden die Objekte untersucht, die beim Hochfahren des Betriebssystems gestartet werden.

Die Aufgaben zur vollständigen und schnellen Untersuchung sind spezifische Aufgaben. Es wird davor gewarnt, die Liste der Untersuchungsobjekte für diese Aufgaben zu ändern.

Jeder Untersuchungsaufgabe wird in einem bestimmten Bereich ausgeführt und kann nach einem festgelegten Zeitplan gestartet werden. Die Parameter von Aufgaben zur Virensuche sind von der Sicherheitsstufe abhängig. Es sind drei vordefinierte Stufen vorgesehen.

Nach dem Start einer Aufgabe zur Virensuche wird im Hauptfenster von Kaspersky Anti-Virus ihr Status im Abschnitt **Untersuchung** im Feld Ende unter dem Namen der gestarteten Aufgabe angezeigt. Beim Fund einer Bedrohung führt die Anwendung eine festgelegte Aktion aus.

Während die Virensuche ausgeführt wird, werden Informationen über ihre Ergebnisse im Bericht von Kaspersky Anti-Virus aufgezeichnet.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen. Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen** aus.



Abbildung 9. Kontextmenü von Microsoft Windows

Außerdem können Sie zum Bericht über die Untersuchung wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung von Aufgaben eingetreten sind, bietet.

SIEHE AUCH

Start der Untersuchungsaufgabe.....	74
Verknüpfung für den Aufgabenstart erstellen	75
Liste der Untersuchungsobjekte erstellen.....	75
Sicherheitsstufe ändern.....	76
Aktion beim Fund einer Bedrohung ändern	76
Typ der zu untersuchenden Objekte ändern	77
Untersuchung optimieren	78
Wechseldatenträger untersuchen.....	78
Untersuchung von zusammengesetzten Dateien	79
Untersuchungstechnologie	79
Untersuchungsmethode ändern	80
Startmodus: Zeitplan erstellen.....	81
Startmodus: Benutzerkonto festlegen.....	81
Besonderheiten beim Start von geplanten Untersuchungsaufgaben.....	82
Standardmäßige Untersuchungseinstellungen wiederherstellen	82

START DER UNTERSUCHUNGSAUFGABE

Für den Start einer Untersuchungsaufgabe stehen folgende Möglichkeiten zur Verfügung:

- aus dem Kontextmenü (s. Abschnitt "Kontextmenü " auf S. [38](#)) von Kaspersky Anti-Virus;
- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)) von Kaspersky Anti-Virus;
- mit einer zuvor hergestellten Verknüpfung (s. S. [75](#)).

Informationen über den Verlauf der Aufgabenausführung werden im Hauptfenster von Kaspersky Anti-Virus angezeigt.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen.



Abbildung 10. Kontextmenü von Microsoft Windows

➡ *Gehen Sie folgendermaßen vor, um eine Aufgabe mit Hilfe einer Verknüpfung zu starten:*

1. Öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Aufgabe durch Doppelklick auf die Verknüpfung. Informationen über die Aufgabenausführung werden im Hauptfenster von Kaspersky Anti-Virus im Abschnitt **Untersuchung** angezeigt.

➡ *Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche aus dem Kontextmenü des Programms zu starten:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
2. Wählen Sie im Kontextmenü den Punkt **Auf Viren untersuchen**.
3. Klicken Sie im folgenden Fenster von Kaspersky Anti-Virus im Abschnitt **Untersuchung** auf die Schaltfläche mit dem Namen der entsprechenden Aufgabe.

Um die vollständige Untersuchung des Computers zu starten, wählen Sie im Kontextmenü den Punkt **Computer vollständig untersuchen** aus. Die vollständige Untersuchung des Computers wird gestartet. Informationen über die Aufgabenausführung werden im Hauptfenster von Kaspersky Anti-Virus im Abschnitt **Untersuchung** angezeigt.

➡ *Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche aus dem Programmhauptfenster zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche mit dem Namen der entsprechenden Aufgabe.

➤ Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche für eine ausgewähltes Objekt aus dem Kontextmenü von Microsoft Windows zu starten:

1. Klicken Sie mit der rechten Maustaste auf den Namen des gewählten Objekts.
2. Wählen Sie im Kontextmenü den Punkt **Auf Viren untersuchen**. Der Fortschritt und das Ergebnis der Aufgabenausführung werden im folgenden Fenster dargestellt.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Zum schnellen Start der Aufgaben zur vollständigen und schnellen Untersuchung ist im Programm die Möglichkeit vorgesehen, eine Verknüpfung anzulegen. So kann die erforderliche Untersuchungsaufgabe gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü zu öffnen.

➤ Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start einer Untersuchungsaufgabe zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem entsprechenden Aufgabennamen (**Schnelle Untersuchung** oder **Vollständige Untersuchung**) auf die Schaltfläche **Verknüpfung erstellen**.
4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig entspricht jeder Aufgabe zur Virensuche eine eigene Liste von Objekten. Zu diesen Objekten können sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, **Mail-Datenbanken**), als auch Objekte anderer Typen (z.B. Netzlaufwerke) gehören. Diese Liste kann geändert werden.

Das hinzugefügte Objekt erscheint sofort in der Liste. Wenn beim Hinzufügen eines Objekts das Kontrollkästchen  **Unterordner einschließen** aktiviert wurde, wird die Untersuchung rekursiv ausgeführt.

Um ein Objekt aus der Liste zu entfernen, verwenden Sie den Link **Löschen**.

Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

Objekte können vorübergehend von der Untersuchung ausgeschlossen werden, ohne aus der Liste gelöscht zu werden. Markieren Sie dazu das Objekt in der Liste und deaktivieren Sie das Kontrollkästchen links vom Namen des Objekts.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden!

➤ Gehen Sie folgendermaßen vor, um für eine Untersuchungsaufgabe eine Liste der Untersuchungsobjekte zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf den Link **Hinzufügen**.

4. Wählen Sie im folgenden Fenster **Untersuchungsobjekt auswählen** ein Objekt aus und klicken Sie auf die Schaltfläche **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

➡ *Gehen Sie folgendermaßen vor, um für eine Aufgabe zur schnellen oder vollständigen Untersuchung eine Liste mit Untersuchungsobjekten zu erstellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite die Aufgabe **Vollständige Untersuchung (Schnelle Untersuchung)** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Untersuchungsobjekte** auf die Schaltfläche **Einstellungen**.
4. Erstellen Sie im folgenden Fenster **<Name der Untersuchungsaufgabe>: Liste der Objekte** mit Hilfe der Links **Hinzufügen**, **Ändern** und **Löschen** eine Liste. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

SICHERHEITSSTUFE ÄNDERN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Untersuchungsparametern verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Bei der Auswahl der Sicherheitsstufe sollten Sie die aktuelle Situation berücksichtigen. Folgende Sicherheitsstufen stehen zur Auswahl:

- **Hoch.** Sie sollte verwendet werden, wenn Sie das Infektionsrisiko für Ihren Computer sehr hoch einschätzen.
- **Empfohlen.** Diese Stufe ist in den meisten Fällen geeignet und wird von den Kaspersky-Lab-Spezialisten empfohlen.
- **Niedrig.** Wenn Sie mit Programmen arbeiten, die den Arbeitsspeicher stark beanspruchen, wählen Sie die niedrige Sicherheitsstufe aus, da die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird.

Wenn keine der vordefinierten Stufen Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen aus.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Stellen Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein.

AKTION BEIM FUND EINER BEDROHUNG ÄNDERN

Beim Fund einer Bedrohung weist Kaspersky Anti-Virus dieser einen der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei der Code eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden.

Wenn Kaspersky Anti-Virus bei einer Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Auf dem Fund einer Bedrohung muss reagiert werden, indem eine Aktion für das Objekt ausgewählt

wird. Standardmäßig ist in Kaspersky Anti-Virus als Aktion für ein gefundenes Objekt die Variante **Aktion erfragen** festgelegt. Sie können die Aktion ändern. Wenn Sie beispielsweise sicher sind, dass versucht werden soll, alle gefundenen Objekte zu desinfizieren, und bei einer Meldung über den Fund eines infizierten oder verdächtigen Objekts nicht jedes Mal die Aktion **Desinfizieren** auswählen möchten, dann legen Sie folgende Aktion fest: **Aktion ausführen. Desinfizieren**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Wenn Sie im automatischen Modus (s. Abschnitt "Schritt 2. Schutzmodus auswählen" auf S. 28) arbeiten, wendet Kaspersky Anti-Virus automatisch die von den Kaspersky-Lab-Fachleuten empfohlene Aktion an, wenn gefährliche Objekte erkannt werden. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige Objekte ist es **Überspringen**.

➡ Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Geben Sie für die ausgewählte Aufgabe im Block **Aktion** die erforderliche Aktion an.

TYP DER ZU UNTERSUCHENDEN OBJEKTE ÄNDERN

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format und die Größe der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen.

Bei der Auswahl des Dateityps sollten folgende Besonderheiten beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. *txt*), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (*exe*, *dll*, *doc*). Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.
- Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn die Variante  **Dateien nach Erweiterung untersuchen** gewählt wurde, wird eine solche Datei bei der Untersuchung übersprungen. Wenn die Variante  **Dateien nach Format untersuchen** gewählt wurde, ignoriert der Dateischutz die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich herausstellen kann, dass die Datei das Format *exe* besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

➡ Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** den gewünschten Parameter.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungszeit verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Anti-Virus erhöhen. Damit nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden: Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann die Untersuchungsdauer für jede Datei beschränkt werden. Nach Ablauf der festgelegten Zeit, wird die Dateiuntersuchung abgebrochen.

➡ *Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen ☒ **Nur neue und veränderte Dateien untersuchen**.

➡ *Gehen Sie folgendermaßen vor, um eine zeitliche Begrenzung für die Untersuchung festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen ☒ **Dateien überspringen, wenn Untersuchungslänger als** und geben Sie im Feld daneben die Untersuchungsdauer an.

WECHSELDATENTRÄGER UNTERSUCHEN

In letzter Zeit treten vermehrt schädliche Objekte auf, die Schwachstellen des Betriebssystems ausnutzen, um sich über lokale Netzwerke und Wechsel Datenträger auszubreiten.

Verwenden Sie eine Funktion, mit der Wechsel Datenträger untersucht werden, wenn sie an den Computer angeschlossen werden. Wählen Sie dazu eine Aktion aus, die Kaspersky Anti-Virus ausführen soll:

- **Nicht untersuchen.** Wenn Wechsel Datenträger an den Computer angeschlossen werden, erfolgt keine Untersuchung.
- **Benutzer fragen.** In der Grundeinstellung werden Sie von Kaspersky Anti-Virus nach dem weiteren Vorgehen gefragt, wenn ein Wechsel Datenträger angeschlossen wird.
- **Vollständige Untersuchung.** Wenn Wechsel Datenträger angeschlossen werden, erfolgt eine vollständige Untersuchung der darauf gespeicherten Dateien. Dabei werden die Parameter der Aufgabe Vollständige Untersuchung verwendet.
- **Schnelle Untersuchung.** Wenn Wechsel Datenträger angeschlossen werden, erfolgt eine Untersuchung aller Objekte. Dabei werden die Parameter der Aufgabe Schnelle Untersuchung verwendet.

➡ *Gehen Sie folgendermaßen vor, um die Option zur Untersuchung von Wechsel Datenträgern zu verwenden, wenn diese an den Computer angeschlossen werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Wählen Sie im Block **Wechseldatenträger beim Anschließen untersuchen** eine Aktion aus und begrenzen Sie bei Bedarf im Feld unten die Größe der zu untersuchenden Laufwerke.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie auswählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben dem Namen des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen (s. S. 78), steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die die festgelegte Größe überschreiten, werden nicht untersucht.

Beim Extrahieren aus Archiven werden Dateien auch dann untersucht, wenn das Kontrollkästchen ☒ **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

➡ Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** den erforderlichen Typ für die zu untersuchenden zusammengesetzten Dateien.

➡ Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im folgenden Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☒ **Große zusammengesetzte Dateien nicht entpacken** und legen Sie darunter im Feld die maximale Größe für zu untersuchende Dateien fest.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich können Sie eine Technologie auswählen, die bei der Untersuchung verwendet werden soll: Folgende Technologien stehen zur Auswahl:

- **iChecker.** Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Objekte ausgeschlossen werden. Das Ausschließen eines Objekts von der Untersuchung erfolgt nach einem speziellen Algorithmus, der das Erscheinungsdatum der Programm-Datenbanken, das Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungsparametern berücksichtigt.

Eine Archivdatei wurde beispielsweise von Kaspersky Anti-Virus untersucht und ihr wurde der Status *virenfrei* zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Objekte angewandt werden, deren Struktur dem Programm bekannt ist (z.B. die Dateiformate exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift.** Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

➡ **Gehen Sie folgendermaßen vor, um die Untersuchungstechnologie für Objekte zu ändern:**

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** den erforderlichen Parameterwert.

UNTERSUCHUNGSMETHODE ÄNDERN

Sie können die Untersuchungsparameter anpassen, die die Ausführlichkeit der Untersuchung beeinflussen. In der Grundeinstellung ist immer der Untersuchungsmodus mit Hilfe der Einträge in Anti-Viren-Datenbanken des Programms aktiviert. Außerdem lassen sich verschiedene Verfahren und Technologien der Untersuchung (s. S. 79) aktivieren.

Der Suchmodus, in dem Kaspersky Anti-Virus ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht, heißt *Signaturanalyse* und wird immer verwendet. Außerdem können Sie die *heuristische Analyse* verwenden. Diese Methode umfasst die Analyse der Aktivität, die ein Objekt im System zeigt. Wenn die erkannte Aktivität als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen.

Zusätzlich kann die Genauigkeitsstufe der heuristischen Analyse ausgewählt werden: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

Neben diesen Untersuchungsmethoden steht noch die Rootkit-Suche zur Verfügung. Ein Rootkit ist eine Kombination von Utilities, die schädliche Programme im Betriebssystem verstecken. Solche Tools dringen in das System ein. Sie tarnen ihre eigene Existenz und verstecken im System die Prozesse, Ordner oder Registrierungsschlüssel anderer Malware, die in der Konfiguration des Rootkits beschrieben ist. Wenn die Rootkit-Suche aktiviert ist, können Sie die Detailstufe für die Suche nach Rootkits auswählen. Aktivieren Sie dazu das Kontrollkästchen **Erweiterte Analyse**. In diesem Fall wird die ausführliche Suche nach solchen Programmen ausgeführt, wobei eine große Anzahl von Objekten unterschiedlicher Typen analysiert wird.

➡ **Gehen Sie folgendermaßen vor, um die erforderlichen Untersuchungsmethoden zu verwenden:**

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).

3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** die gewünschten Parameterwerte.

STARTMODUS: ZEITPLAN ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Untersuchungsaufgabe angelegt werden.

Die wichtigste Einstellung ist die Frequenz, mit der der Aufgabenstart erfolgen soll. Dazu ist es erforderlich, die Zeitplanparameter für die gewählte Variante anzugeben.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start automatisch zum nächstmöglichen Zeitpunkt erfolgt.

➡ *Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Variante **Manuell** aus, wenn Sie die Untersuchungsaufgabe zu einem geeigneten Zeitpunkt auf Befehl starten möchten. Damit die Aufgabe regelmäßig ausgeführt wird, wählen Sie die Variante **Nach Zeitplan** aus und legen Sie einen Zeitplan für den Aufgabenstart fest.

➡ *Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** das Kontrollkästchen ☒ **Übersprungene Aufgabe starten**.

STARTMODUS: BENUTZERKONTO FESTLEGEN

Sie können das Benutzerkonto festlegen, mit dessen Rechten die Suche ausgeführt werden soll.

➡ *Gehen Sie folgendermaßen vor, um ein Benutzerkonto festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen ☒ **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

BESONDERHEITEN BEIM START VON GEPLANTEN UNTERSUCHUNGSAUFGABEN

Alle Untersuchungsaufgaben können auf Befehl oder nach einem festgelegten Zeitplan gestartet werden.

Für Aufgaben, die nach einem festgelegten Zeitplan gestartet werden, können Sie eine zusätzliche Option verwenden: *Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv oder Computer nicht blockiert ist*. Diese Option erlaubt es, den Start einer Aufgabe zurückzustellen, bis der Benutzer seine Arbeit auf dem Computer beendet hat. Dadurch wird verhindert, dass eine Untersuchungsaufgabe Computerressourcen verbraucht, während diese für andere Aufgaben benötigt werden.

- *Gehen Sie folgendermaßen vor, damit die Untersuchung erst gestartet wird, nachdem der Benutzer seine Arbeit beendet hat:*
 1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
 2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
 3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
 4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** das Kontrollkästchen ☒ **Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv oder Computer nicht blockiert ist**.

STANDARMÄßIGE UNTERSUCHUNGSEINSTELLUNGEN WIEDERHERSTELLEN

Während der Konfiguration der Parameter für die Aufgabenausführung können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

- *Gehen Sie folgendermaßen vor, um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,*
 1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
 2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**).
 3. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf die Schaltfläche **Standard**.

SUCHE NACH SCHWACHSTELLEN

Die Aufgabe zur Schwachstellen-Suche umfasst eine Diagnose der Systemsicherheit und die Suche nach potentiellen Schwachstellen, die Angreifer gewöhnlich ausnutzen, um Schaden anzurichten.

Im Rahmen der Schwachstellen-Suche wird das System analysiert und es wird in den Einstellungen des Betriebssystems und des Browsers nach Anomalien und Beschädigungen gesucht. Die Sicherheitsdiagnose berücksichtigt unter anderem folgende Aspekte: Suche nach Rootkits (Programme zur heimlichen Kontrolle eines gehackten Systems), Suche nach Schwachstellen in Diensten und Parametern, Sammeln von Informationen über Prozesse, Treiber usw.

Die Systemdiagnose kann eine gewisse Zeit beanspruchen. Anschließend werden die gesammelten Informationen analysiert. Das Ziel der Analyse besteht darin, die gefundenen Sicherheitsprobleme hinsichtlich ihrer Gefährlichkeit für das System zu bewerten.

Alle Probleme, die bei der Systemanalyse gefunden wurden, werden im Hinblick auf die von ihnen für das System ausgehende Gefahr eingeteilt. Für jede Gruppe von Problemen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, mit denen die Schwachstellen und kritischen Punkte im System behoben werden können. Die Probleme und die entsprechenden Aktionen sind in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Probleme beheben, die eine ernsthafte Sicherheitsbedrohung darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe auszuführen.
- *Empfohlene Aktionen* dienen zum Beheben von Problemen, die ein potentielles Risiko darstellen können. Es wird empfohlen, auch alle Aktionen dieser Gruppe auszuführen.
- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Probleme zu beheben, die die Computersicherheit in Zukunft bedrohen können.

Das Ergebnis der Suche nach potentiellen Schwachstellen im Betriebssystem und in den auf dem Computer installierten Anwendungen besteht in direkten Links zu kritischen Patches (Updates für Anwendungen).

Nach dem Start der Aufgabe Suche nach Schwachstellen (s. S. [83](#)) wird der Fortschritt im Programmhauptfenster und im Fenster **Suche nach Schwachstellen** im Feld **Ende** angezeigt. Die bei der Untersuchung im System und in Programmen gefundenen Schwachstellen werden im gleichen Fenster auf den Registerkarten **Systemschwachstellen** und **Programme mit Schwachstellen** angezeigt.

Während die Virensuche ausgeführt wird, werden Informationen über ihre Ergebnisse im Bericht von Kaspersky Anti-Virus aufgezeichnet.

Analog zu den Aufgaben zur Virensuche kann auch für die Schwachstellen-Suche im Abschnitt **Suche nach Schwachstellen** des Programmkonfigurationsfensters einen Startzeitplan (s. S. [85](#)) erstellt und eine Liste der Untersuchungsobjekte (s. S. [84](#)) angelegt werden. In der Grundeinstellung sind die auf dem Computer installierten Anwendungen als Untersuchungsobjekt ausgewählt.

SIEHE AUCH

Aufgabe zur Suche nach Schwachstellen starten	83
Verknüpfung für den Aufgabenstart erstellen	84
Liste der Untersuchungsobjekte erstellen.....	84
Startmodus: Zeitplan erstellen.....	85
Startmodus: Benutzerkonto festlegen.....	85

AUFGABE ZUR SUCHE NACH SCHWACHSTELLEN STARTEN

Für den Start der Aufgabe zur Schwachstellen-Suche stehen folgende Möglichkeiten zur Verfügung:

- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)) von Kaspersky Anti-Virus;
- mit einer zuvor hergestellten Verknüpfung (s. S. [84](#)).

Die Daten zur Aufgabenausführung werden im Hauptfenster von Kaspersky Anti-Virus und im Fenster **Suche nach Schwachstellen** angezeigt.

➡ *Gehen Sie folgendermaßen vor, um eine Aufgabe mit Hilfe einer Verknüpfung zu starten:*

1. Öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Aufgabe durch Doppelklick auf die Verknüpfung. Der Ausführungsfortschritt der Aufgabe wird im Programmhauptfenster dargestellt.

➤ Gehen Sie folgendermaßen vor, um die Aufgabe zur Schwachstellen-Suche aus dem Programmfenster zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf die Schaltfläche **Fenster zur Suche nach Schwachstellen öffnen**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Suche nach Schwachstellen ausführen**. Informationen über die Aufgabenausführung werden im Feld **Ende** angezeigt. Um die Aufgabenausführung abubrechen, klicken Sie erneut auf die Schaltfläche.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Zum schnellen Start einer Aufgabe zur Suche nach Schwachstellen ist im Programm die Möglichkeit vorgesehen, eine Verknüpfung zu erstellen. So kann eine Aufgabe gestartet werden, ohne das Programmhauptfenster zu öffnen.

➤ Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start der Aufgabe zur Suche nach Schwachstellen zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem Aufgabennamen (**Suche nach Schwachstellen**) auf die Schaltfläche **Verknüpfung erstellen**.
4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig verfügt die Aufgabe zur Schwachstellen-Suche über eine eigene Liste von Untersuchungsobjekten. Zu diesen Objekten gehören das Betriebssystem und die auf dem Computer installierten Programme. Es können auch zusätzliche Untersuchungsobjekte angegeben werden: sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, **Mail-Datenbanken**), als auch Objekte anderer Typen (z.B. Netzlaufwerke).

Das hinzugefügte Objekt erscheint sofort in der Liste. Wenn beim Hinzufügen eines Objekts das Kontrollkästchen ☒ **Unterordner einschließen** aktiviert wurde, wird die Untersuchung rekursiv ausgeführt. Objekte, die manuell hinzugefügt wurden, werden ebenfalls der Virusuntersuchung unterzogen.

Um ein Objekt aus der Liste zu entfernen, verwenden Sie den Link **Löschen**.

Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

Objekte können vorübergehend von der Untersuchung ausgeschlossen werden, ohne aus der Liste gelöscht zu werden. Markieren Sie dazu das Objekt in der Liste und deaktivieren Sie das Kontrollkästchen links vom Namen des Objekts.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden!

➤ Gehen Sie folgendermaßen vor, um eine Liste der Objekte für die Aufgabe zur Schwachstellen-Suche zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Virensuche** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Untersuchungsobjekte** auf die Schaltfläche **Einstellungen**.
4. Erstellen Sie im folgenden Fenster **Suche nach Schwachstellen: Liste der Objekte** mit Hilfe der Links **Hinzufügen**, **Ändern** und **Löschen** eine Liste. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

STARTMODUS: ZEITPLAN ERSTELLEN

Für die Aufgabe zur Schwachstellen-Suche kann ein Zeitplan für den automatischen Aufgabenstart erstellt werden.

Die wichtigste Einstellung ist die Frequenz, mit der die Aufgabe ausgeführt werden soll.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start automatisch zum nächstmöglichen Zeitpunkt erfolgt.

➡ *Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Virensuche** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Variante **Manuell** aus, wenn Sie die Untersuchungsaufgabe zu einem geeigneten Zeitpunkt auf Befehl starten möchten. Damit die Aufgabe regelmäßig ausgeführt wird, wählen Sie die Variante **Nach Zeitplan** aus und legen Sie einen Zeitplan für den Aufgabenstart fest.

➡ *Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Virensuche** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** das Kontrollkästchen ☒ **Übersprungene Aufgabe starten**.

STARTMODUS: BENUTZERKONTO FESTLEGEN

Sie können das Benutzerkonto festlegen, mit dessen Rechten die Suche nach Schwachstellen ausgeführt werden soll.

➡ *Gehen Sie folgendermaßen vor, um ein Benutzerkonto festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Virensuche** die Aufgabe **Suche nach Schwachstellen** aus.
3. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf die Schaltfläche **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen ☒ **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

UPDATE

Eine Voraussetzung für die Sicherheit Ihres Computers besteht darin, den Schutz auf dem neusten Stand zu halten. Jeden Tag tauchen neue Viren, trojanische und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden. Informationen über Bedrohungssignaturen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Anti-Virus enthalten. Deshalb stellt die regelmäßige Aktualisierung der Datenbanken einen sehr wichtigen Sicherheitsfaktor dar.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

- Datenbanken für Kaspersky Anti-Virus.

Der Schutz der Informationen auf Ihrem Computer basiert auf Datenbanken, die Beschreibungen von Bedrohungssignaturen und Netzwerkangriffen, sowie entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

Gemeinsam mit den Datenbanken von Kaspersky Anti-Virus werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

- Programm-Module.

Neben den Datenbanken von Kaspersky Anti-Virus können auch die Programm-Module aktualisiert werden. Updatepakete beheben Schwachstellen von Kaspersky Anti-Virus, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Die wichtigste Updatequelle für Kaspersky Anti-Virus sind spezielle Updateserver von Kaspersky Lab.

Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn die Proxyserver-Einstellungen nicht automatisch ermittelt werden, passen Sie die Parameter der Verbindung mit dem Proxyserver an.

Bei der Aktualisierung werden die Programm-Module und Datenbanken auf Ihrem Computer mit den auf der Updatequelle vorhandenen verglichen. Wenn auf Ihrem Computer die aktuelle Version der Datenbanken und Module installiert ist, erscheint auf dem Bildschirm eine Meldung darüber, dass der Schutz auf Ihrem Computer aktuell ist. Wenn Datenbanken und Module nicht aktuell sind, wird nur der fehlende Teil der Updates auf Ihrem Computer installiert. Datenbanken und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Wenn die Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Bevor die Datenbanken aktualisiert werden, legt Kaspersky Anti-Virus eine Sicherungskopie davon an. Bei Bedarf können Sie zur vorhergehenden Version der Datenbanken zurückkehren.

Die Option zum Rollback des Updates ist beispielsweise erforderlich, wenn Sie die Datenbanken aktualisiert haben und diese bei der Arbeit beschädigt wurden. Es ist möglich, zu der vorherigen Variante der Datenbanken zurückzukehren und die Aktualisierung später erneut zu versuchen.

Synchron zur Aktualisierung von Kaspersky Anti-Virus können Sie das Kopieren der heruntergeladenen Updates in eine lokale Quelle ausführen. Dieser Dienst erlaubt es, die Datenbanken und Module des Programms auf Netzwerkcomputern zu aktualisieren und dabei Netzwerkverkehr einzusparen.

Zusätzlich kann der Modus für den automatischen Start des Updates angepasst werden.

Im Abschnitt **Update** des Programmhauptfensters werden Informationen über den aktuellen Zustand der Datenbanken von Kaspersky Anti-Virus angezeigt:

- Datum und Uhrzeit des Erscheinens
- Anzahl und Zusammensetzung der Einträge in den Datenbanken.
- Status der Datenbanken (aktuell, veraltet oder beschädigt)

Sie können zum Bericht über das Update wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung der Updateaufgabe eingetreten sind, bietet (der Link **Bericht** im oberen Bereich des Fensters). Außerdem können Sie auf der Seite www.kaspersky.com einen Überblick über die Virenaktivität erhalten (Link **Überblick über die Virenaktivität**).

IN DIESEM ABSCHNITT

Update starten	88
Rollback zum vorherigen Update	89
Updatequelle auswählen	89
Proxyserver verwenden	90
Regionsoptionen	90
Aktionen nach dem Update	90
Update aus einem lokalen Ordner	91
Startmodus für die Updateaufgabe ändern	91
Updatestart mit den Rechten eines anderen Benutzers	92

UPDATE STARTEN

Sie können das Update von Kaspersky Anti-Virus jederzeit starten. Es erfolgt aus der von Ihnen ausgewählten Updatequelle (s. Abschnitt "Updatequelle auswählen" auf S. [89](#)).

Das Update von Kaspersky Anti-Virus kann auf zwei Arten gestartet werden:

- aus dem Kontextmenü (s. Abschnitt "Kontextmenü " auf S. [38](#)).
- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. [39](#)).

Die Informationen über den Updateprozess werden im Abschnitt **Update** des Programmhauptfensters angezeigt.

➡ *Gehen Sie folgendermaßen vor, um das Update von Kaspersky Anti-Virus aus dem Kontextmenü zu starten:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
2. Wählen Sie im Kontextmenü den Punkt **Update** aus.

➡ *Gehen Sie folgendermaßen vor, um das Update aus dem Hauptfenster von Kaspersky Anti-Virus zu starten,*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie auf die Schaltfläche **Update ausführen**. Der Ausführungsfortschritt der Aufgabe wird im Programmhauptfenster dargestellt.

ROLLBACK ZUM VORHERIGEN UPDATE

Jedes Mal, wenn Sie das Update starten, erstellt Kaspersky Anti-Virus zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt danach mit der Aktualisierung. Dadurch wird Ihnen erlaubt, zur Verwendung der vorherigen Datenbanken zurückzukehren, wenn das Update erfolglos war.

Die Rollback-Funktion ist beispielsweise nützlich, wenn die Datenbanken teilweise beschädigt wurden. Lokale Datenbanken können entweder von einem Benutzer oder von einem bösartigen Programm beschädigt werden. Eine Beschädigung ist nur möglich, wenn der Selbstschutz (s. Abschnitt "Selbstschutz von Kaspersky Anti-Virus" auf S. [101](#)) von Kaspersky Anti-Virus deaktiviert wurde. Sie können zu den vorherigen Datenbanken zurückkehren und die Aktualisierung später erneut versuchen.

➡ *Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie auf die Schaltfläche **Rollback zu den vorherigen Datenbanken**.

UPDATEQUELLE AUSWÄHLEN

Eine *Updatequelle* ist eine Ressource, die Updates der Datenbanken und der Module für Kaspersky Anti-Virus enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner dienen.

Als primäre Updatequelle gelten die Kaspersky-Lab-Updateserver. Dabei handelt es sich um spezielle Internetseiten, auf denen Updates der Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Updates, die sich auf einem Wechseldatenträger befinden, können Sie auf einer ftp- oder http-Seite oder in einem lokalen oder Netzwerkordner speichern.

Geben Sie zur Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates für die Programm-Module erhalten möchten.

In der Grundeinstellung enthält die Liste nur die Kaspersky-Lab-Updateserver.

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift das Kaspersky Anti-Virus bei der Aktualisierung genau nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle.

➡ *Gehen Sie folgendermaßen vor, um eine Updatequelle auszuwählen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Updatequelle auswählen** eine ftp- oder http-Seite oder geben Sie ihre IP-Adresse, den symbolischen Namen oder die URL-Adresse an.

PROXYSERVER VERWENDEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die Parameter anzupassen.

➤ *Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie auf der Registerkarte **Quelle** auf die Schaltfläche **Proxyserver**.
5. Passen Sie im folgenden Fenster **Proxyserver-Einstellungen** die Parameter für den Proxyserver an.

REGIONSOPTIONEN

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, kann der für Sie günstigste Standort des Servers für den Update-Download ausgewählt werden. Kaspersky Lab verfügt in mehreren Ländern der Erde über Server. Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen.

➤ *Gehen Sie folgendermaßen vor, um den nächstliegenden Server auszuwählen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Updatequelle** im Block **Regionsoptionen** das Kontrollkästchen  **Aus der Liste auswählen** und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gerade aufhalten.

Wenn die Variante  **Automatisch ermitteln** gewählt wurde, werden beim Update Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

AKTIONEN NACH DEM UPDATE

In Kaspersky Anti-Virus können die Aktionen festgelegt werden, die automatisch nach dem Update ausgeführt werden sollen. Folgende Aktionen sind möglich:

- **Quarantäne Dateien untersuchen.** In die Quarantäne werden Objekte verschoben, bei deren Untersuchung nicht genau festgestellt werden konnte, von welchen schädlichen Programmen sie infiziert sind. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken aktualisiert wurden. Deshalb untersucht das Programm die Quarantäneobjekte nach jedem Update. Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich ihr Status ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.
- **Updates in folgenden Ordner kopieren.** Wenn Computer zu einem lokalen Netzwerk zusammengeschlossen sind, ist es überflüssig, die Updates für jeden Computer einzeln herunterzuladen und zu installieren, weil dadurch eine erhöhte Netzwerkbelastung verursacht würde. Sie können die Funktion zur Update-Verteilung verwenden, mit dem der Netzwerkverkehr verringert werden kann, weil Updates nur einmal heruntergeladen werden müssen.

➡ *Gehen Sie folgendermaßen vor, damit die Dateien, die sich in der Quarantäne befinden, nach dem Update untersucht werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen ☒ **Quarantänedateien nach jedem Update untersuchen**.

UPDATE AUS EINEM LOKALEN ORDNER

Die Update-Verteilung aus einem lokalen Ordner wird folgendermaßen organisiert:

1. Ein Computer des Netzwerks lädt das Paket mit den Updates für Kaspersky Anti-Virus von den Kaspersky-Lab-Webservern im Internet oder einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.
2. Die übrigen Netzwerkcomputer verwenden den gemeinsamen Ordner, um die Updates von Kaspersky Anti-Virus herunterzuladen.

➡ *Gehen Sie folgendermaßen vor, um den Modus für die Update-Verteilung zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen ☒ **Updates in folgenden Ordner kopieren** und geben Sie darunter im Feld den Pfad des gemeinsamen Ordners an, in dem die heruntergeladenen Updates abgelegt werden sollen. Der Pfad kann auch im Fenster, das mit der Schaltfläche **Durchsuchen** geöffnet wird, gewählt werden.

➡ *Damit das Update aus dem gewählten gemeinsamen Ordner erfolgt, nehmen Sie auf allen Computern des Netzwerks folgende Einstellungen vor:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Updatequelle** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Updatequelle auswählen** den Ordner und geben Sie im Feld **Quelle** seinen vollständigen Pfad an.
6. Deaktivieren Sie auf der Registerkarte **Quelle** das Kontrollkästchen ☒ **Kaspersky-Lab-Updateserver**.

STARTMODUS FÜR DIE UPDATEAUFGABE ÄNDERN

Der Startmodus für das Update von Kaspersky Anti-Virus wird im Konfigurationsassistenten von Kaspersky Anti-Virus festgelegt (s. Abschnitt "Schritt 3. Programm-Update anpassen" auf S. 29) auswählen. Später kann der Startmodus für das Update geändert werden.

Für den Start der Updateaufgabe stehen folgende Modi zur Auswahl:

-  **Automatisch.** Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates gefunden werden, lädt das Programm sie herunter und installiert sie auf dem Computer.
-  **Nach Zeitplan** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet.
-  **Manuell.** In diesem Fall starten Sie das Update von Kaspersky Anti-Virus auf Befehl.

➡ *Gehen Sie folgendermaßen vor, um den Startmodus für die Updateaufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** einen Startmodus für die Updateaufgabe. Wenn der Modus  **Nach Zeitplan** gewählt wurde, legen Sie einen Zeitplan an.

Wenn der Start einer Aufgabe aus einem bestimmten Grund übersprungen wurde (wenn beispielsweise der Computer ausgeschaltet war), können Sie festlegen, dass die übersprungene Aufgabe automatisch gestartet wird, sobald dies möglich ist. Aktivieren Sie dazu  im unteren Bereich des Fensters das Kontrollkästchen **Übersprungene Aufgaben starten**. Dieses Kontrollkästchen steht für alle Zeitplanvarianten zur Verfügung, außer für **Stunden**, **Minuten** und **Nach dem Programmstart**.

UPDATESTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Das Update wird standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Das Update für Kaspersky Anti-Virus kann aber aus einer Quelle (z.B. Netzwerkordner, der Updates enthält) erfolgen, auf die Sie keinen Zugriff besitzen oder für die Sie nicht über Rechte eines autorisierten Benutzers für den Proxyserver verfügen. Sie können das Update von Kaspersky Anti-Virus unter dem Namen eines Benutzers starten, der über die erforderlichen Privilegien verfügt.

➡ *Gehen Sie folgendermaßen vor, um das Update mit den Rechten eines anderen Benutzers zu starten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Klicken Sie im Block **Startmodus** auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen  **Aufgabe starten mit Rechten des anderen Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

PROGRAMMPARAMETER ANPASSEN

Das Programmkonfigurationsfenster dient dem schnellen Zugriff auf die wichtigsten Einstellungen von Kaspersky Anti-Virus.

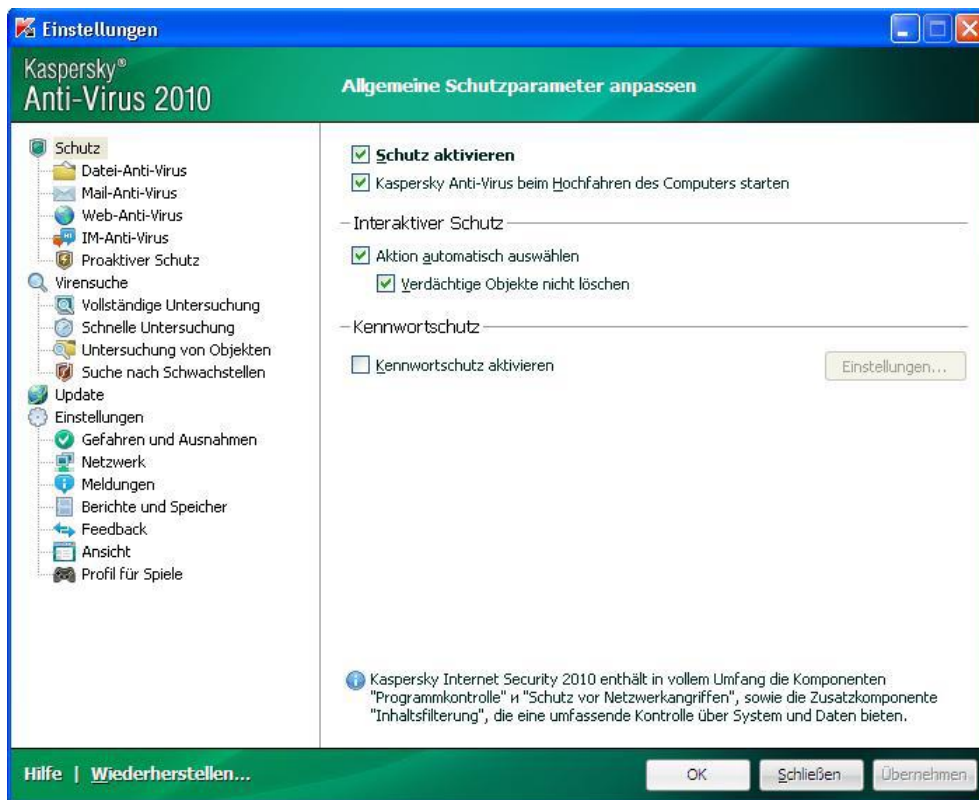


Abbildung 11. Programmkonfigurationsfenster

Das Konfigurationsfenster besteht aus zwei Teilen:

- Die linke Seite des Fensters bietet Zugriff auf die Komponenten von Kaspersky Anti-Virus, auf Untersuchungs- und Updateaufgaben und andere Funktionen.
- Die rechte Seite des Fensters enthält eine Liste von Parametern für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

Zum Öffnen des Fensters gibt es folgende Möglichkeiten:

- aus dem Hauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Anti-Virus" auf S. 39) von Kaspersky Anti-Virus. Klicken Sie dazu im oberen Bereich des Hauptfensters auf den Link **Einstellungen**.

- aus dem Kontextmenü (s. Abschnitt "Kontextmenü " auf S. [38](#)). Wählen Sie dazu im Kontextmenü des Programms den Punkt **Einstellungen** aus.



Abbildung 12. Kontextmenü

IN DIESEM ABSCHNITT

Schutz	94
Datei-Anti-Virus	96
Mail-Anti-Virus	97
Web-Anti-Virus	98
IM-Anti-Virus	99
Proaktiver Schutz	99
Untersuchung	100
Update	101
Einstellungen	101

SCHUTZ

Im Fenster **Schutz** können Sie folgende Zusatzfunktionen von Kaspersky Anti-Virus verwenden:

- Schutz von Kaspersky Anti-Virus aktivieren / deaktivieren (s. S. [94](#)).
- Kaspersky Anti-Virus beim Hochfahren des Betriebssystems starten (s. S. [95](#)).
- Interaktiven Schutzmodus verwenden (s. S. [95](#)).
- Kontrolle des Zugriffs auf Kaspersky Anti-Virus (s. S. [96](#)).

COMPUTERSCHUTZ AKTIVIEREN / DEAKTIVIEREN

Kaspersky Anti-Virus wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten sind aktiv.

Sie können den Schutz, der von Kaspersky Anti-Virus gewährleistet wird, vollständig oder teilweise deaktivieren.

Die Kaspersky-Lab-Spezialisten **warnen ausdrücklich davor, den Schutz zu deaktivieren**, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Wenn der Schutz deaktiviert wird, wird die Arbeit aller Komponenten beendet. Darüber informieren folgende Merkmale:

- Das inaktive (graue) (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 37) im Infobereich der Taskleiste.
- Die rote Farbe des Sicherheitsindikators.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky Anti-Virus aus.

➡ *Gehen Sie folgendermaßen vor, um den Schutz vollständig auszuschalten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Deaktivieren Sie das Kontrollkästchen ☒ **Schutz aktivieren**.

KASPERSKY ANTI-VIRUS BEIM HOCHFAHREN DES BETRIEBSSYSTEMS STARTEN

Wenn es erforderlich ist, die Arbeit von Kaspersky Anti-Virus vollständig zu beenden, wählen Sie im Kontextmenü (s. Abschnitt "Kontextmenü" auf S. 38) von Kaspersky Anti-Virus den Punkt **Beenden** aus. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt. Das bedeutet, Ihr Computer ist ungeschützt.

Der Computerschutz kann wieder aktiviert werden, indem Kaspersky Anti-Virus aus dem **Startmenü** → **Programme** → **Kaspersky Anti-Virus 2010** @ **Kaspersky Anti-Virus 2010** gestartet wird.

Außerdem kann der Schutz nach dem Neustart des Betriebssystems automatisch gestartet werden.

➡ *Gehen Sie folgendermaßen vor, um diesen Modus zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Aktivieren Sie das Kontrollkästchen ☒ **Kaspersky Anti-Virus beim Hochfahren des Computers starten**.

INTERAKTIVEN SCHUTZMODUS VERWENDEN

Kaspersky Anti-Virus bietet zwei Modi für die Kooperation mit dem Benutzer:

- *Interaktiver Schutzmodus.* Kaspersky Anti-Virus benachrichtigt den Benutzer über alle gefährlichen und verdächtigen Ereignisse im System. In diesem Modus muss der Benutzer selbständig entscheiden, ob bestimmte Aktionen erlaubt oder verboten werden sollen.
- *Automatischer Schutzmodus.* Kaspersky Anti-Virus führt automatisch die von den Kaspersky-Lab-Experten empfohlene Aktion aus, wenn gefährliche Ereignisse eintreten.

➡ Gehen Sie folgendermaßen vor, um den automatischen Schutzmodus zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Aktivieren Sie im Block **Interaktiver Schutz** das Kontrollkästchen ☒ **Aktion automatisch auswählen**. Wenn verdächtige Objekte bei der Arbeit im automatischen Modus nicht gelöscht werden sollen, dann aktivieren Sie das Kontrollkästchen ☒ **Verdächtige Objekte nicht löschen**.

KONTROLLE DES ZUGRIFFS AUF KASPERSKY ANTI-VIRUS

Es kann sein, dass ein PC von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern völlig unterschiedlich sind. Der ungehinderte Zugriff auf Kaspersky Anti-Virus und dessen Einstellungen kann das Sicherheitsniveau des Computers stark einschränken.

Verwenden Sie ein Kennwort für den Zugriff auf Kaspersky Anti-Virus, um die Sicherheit des Computers zu erhöhen. Sie können entweder alle Operationen mit Kaspersky Anti-Virus blockieren (unter Ausnahme der Arbeit mit Meldungen über den Fund gefährlicher Objekte) oder das Ausführen folgender Aktionen untersagen:

- Programmparameter ändern.
- Programm beenden.

➡ Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky Anti-Virus durch ein Kennwort zu schützen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
3. Aktivieren Sie im Block **Kennwortschutz** das Kontrollkästchen ☒ **Kennwortschutz aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Geben Sie im folgenden Fenster **Kennwortschutz** das Kennwort an und legen Sie den Bereich fest, für den die Zugriffsbeschränkung gelten soll. Beim Versuch eines beliebigen Benutzers Ihres Computers, die von Ihnen festgelegten Aktionen auszuführen, wird Kaspersky Anti-Virus nun immer das Kennwort abfragen.

DATEI-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente Datei-Anti-Virus (s. Abschnitt "Schutz für das Dateisystem des Computers" auf S. [42](#)) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Datei-Anti-Virus deaktivieren.
- Sicherheitsstufe ändern (s. S. [44](#)).
- Aktion für erkannte Objekte ändern (s. S. [44](#)).
- Schutzbereich festlegen (s. S. [45](#)).
- Untersuchung optimieren (s. S. [47](#)).
- Untersuchung von zusammengesetzten Dateien anpassen (s. S. [47](#)).
- Untersuchungsmodus ändern (s. S. [48](#)).

- heuristische Analyse verwenden (s. S. [46](#)).
- Komponente anhalten (s. S. [49](#)).
- Untersuchungstechnologie auswählen (s. S. [48](#)).
- Standard-Schutzeinstellungen wiederherstellen (s. S. [51](#)), wenn sie geändert wurden.

➡ *Gehen Sie folgendermaßen vor, um Datei-Anti-Virus zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen ☒ **Datei-Anti-Virus aktivieren**.

➡ *Gehen Sie folgendermaßen vor, um zu den Einstellungen für Datei-Anti-Virus zu gelangen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus** aus.
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Datei-Anti-Virus anzupassen.

MAIL-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente Mail-Anti-Virus (s. Abschnitt "E-Mail-Schutz" auf S. [52](#)) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Mail-Anti-Virus deaktivieren.
- Sicherheitsstufe ändern (s. S. [53](#)).
- Aktion für erkannte Objekte ändern (s. S. [54](#)).
- Schutzbereich festlegen (s. S. [55](#)).
- heuristische Analyse verwenden (s. S. [57](#)).
- Untersuchung von zusammengesetzten Dateien anpassen (s. S. [57](#)).
- Filterbedingungen für an E-Mails angehängte Objekte anpassen. (s. S. [57](#)).
- Standard-Schutzeinstellungen wiederherstellen (s. S. [58](#)).

➡ *Gehen Sie folgendermaßen vor, um Mail-Anti-Virus zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen ☒ **Mail-Anti-Virus aktivieren**.

➡ *Gehen Sie folgendermaßen vor, um zu den Einstellungen für Mail-Anti-Virus zu gelangen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus** aus.
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Mail-Anti-Virus anzupassen.

WEB-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente Web-Anti-Virus (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. 59) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Web-Anti-Virus deaktivieren.
- Sicherheitsstufe ändern (s. S. 61).
- Aktion für erkannte Objekte ändern (s. S. 61).
- Schutzbereich festlegen (s. S. 62).
- Untersuchungsmethoden ändern (s. S. 62).
- Modul für Link-Untersuchung verwenden (s. S. 63).
- Untersuchung optimieren (s. S. 64).
- heuristische Analyse verwenden (s. S. 64).
- Standardparameter für den Web-Schutz wiederherstellen (s. S. 65).

➡ *Gehen Sie folgendermaßen vor, um Web-Anti-Virus zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen ☒ **Web-Anti-Virus aktivieren**.

➡ *Gehen Sie folgendermaßen vor, um zu den Einstellungen für Web-Anti-Virus zu gelangen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Web-Anti-Virus** aus.
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Web-Anti-Virus anzupassen.

IM-ANTI-VIRUS

Im Fenster sind die Parameter für die Komponente IM-Anti-Virus (s. Abschnitt "Schutz für den Datenverkehr von Instant-Messengern" auf S. [66](#)) angeordnet. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- IM-Anti-Virus deaktivieren.
- Schutzbereich festlegen (s. S. [67](#)).
- Untersuchungsmethode ändern (s. S. [67](#)).
- heuristische Analyse verwenden (s. S. [68](#)).

➡ *Gehen Sie folgendermaßen vor, um IM-Anti-Virus zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen ☒ **IM-Anti-Virus aktivieren**.

➡ *Gehen Sie folgendermaßen vor, um zu den Einstellungen für IM-Anti-Virus zu gelangen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **IM-Anti-Virus** aus.
3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

PROAKTIVER SCHUTZ

Dieses Fenster enthält die Parameter der Komponente Proaktiver Schutz. Durch eine Veränderung der Parameterwerte, können Sie folgende Aktionen ausführen:

- Proaktiven Schutz deaktivieren.
- Liste der gefährlichen Aktivitäten verwalten.
- Reaktion des Programms auf gefährliche Aktivität im System ändern (s. S. [70](#)).
- Gruppe mit vertrauenswürdigen Programmen erstellen (s. S. [71](#)).
- System-Benutzerkonten kontrollieren (s. S. [71](#)).

➡ *Gehen Sie folgendermaßen vor, um den Proaktiven Schutz zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen ☒ **Proaktiven Schutz aktivieren**.

➡ *Gehen Sie folgendermaßen vor, um zu den Einstellungen für den Proaktiven Schutz zu gelangen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz** die Komponente **Proaktiver Schutz** aus.
3. Passen Sie die Parameter der Komponente auf der rechten Seite des Fensters entsprechend an.

UNTERSUCHUNG

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für jede Aufgabe festgelegt werden.

Die Spezialisten von Kaspersky Lab haben Aufgaben für die Virensuche und für die Suche nach Schwachstellen vordefiniert. Zu den Aufgaben für die Virensuche gehören:

- **Objekte untersuchen.** Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.
- **Vollständige Untersuchung.** Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Schnelle Untersuchung.** Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Im Konfigurationsfenster können Sie für jede Untersuchungsaufgabe folgende Aktionen ausführen:

- Sicherheitsstufe auswählen, auf deren Basis die Aufgabe ausgeführt werden soll.
- Aktion auswählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird.
- Zeitplan für den automatischen Aufgabenstart erstellen.
- Liste der Untersuchungsobjekte erstellen (für die Aufgaben zur schnellen und vollständigen Untersuchung).
- Typen der Dateien, die der Virenanalyse unterzogen werden, festlegen.
- Parameter für die Untersuchung von zusammengesetzten Dateien festlegen.
- Methoden und Technologien für die Untersuchung auswählen.

Im Abschnitt **Virensuche** lassen sich die Parameter für die automatische Untersuchung von Wechseldatenträgern bei deren Verbindung mit dem Computer angeben und Verknüpfungen für einen schnellen Start der Aufgaben Virenuntersuchung und Schwachstellensuche herstellen.

Im Konfigurationsfenster der Aufgabe zur Schwachstellen-Suche können Sie:

- Zeitplan für den automatischen Aufgabenstart erstellen.
- Liste der Untersuchungsobjekte erstellen.

➡ *Gehen Sie folgendermaßen vor, um die Aufgabenparameter anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Virensuche** die erforderliche Aufgabe aus (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten**, **Suche nach Schwachstellen**).

3. Nehmen Sie auf der rechten Seite des Fensters die entsprechenden Einstellungen vor.

UPDATE

Das Update von Kaspersky Anti-Virus wird nach den folgenden Parametern ausgeführt.

Im Konfigurationsfenster für die Updateaufgabe können Sie folgende Aktionen ausführen:

- Adresse der Quelle ändern, von der die Updates des Programms kopiert und installiert werden.
- Den Modus bestimmen, in dem der Updateprozess für das Programm gestartet wird.
- Zeitplan für Start der Aufgabe erstellen.
- Benutzerkonto, in dessen Namen das Update gestartet wird, angeben.
- Aktionen, die nach dem Programm-Update ausgeführt werden sollen, angeben.

➡ *Gehen Sie folgendermaßen vor, um zur Konfiguration der Updateparameter zu wechseln:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update** aus.
3. Wählen Sie auf der rechten Seite des Fensters den erforderlichen Startmodus aus. Geben Sie im Block **Erweitert** weitere Aufgabenparameter an.

EINSTELLUNGEN

Im Fenster **Einstellungen** können Sie folgende Zusatzfunktionen von Kaspersky Anti-Virus verwenden:

- Selbstschutz für Kaspersky Anti-Virus (s. S. [101](#)).
- Technologie der aktiven Desinfektion verwenden (s. S. [102](#)).
- Dienst zum Sparen von Akkustrom (s. S. [102](#)).
- Zurückgestellte Ausführung von Aufgaben zur Virensuche bei verlangsamer Arbeit anderer Programme (s. S. [103](#)).
- Funktionsparameter für Kaspersky Anti-Virus exportieren / importieren (s. S. [103](#)).
- Standardmäßige Funktionsparameter für Kaspersky Anti-Virus wiederherstellen (s. S. [104](#)).

SELBSTSCHUTZ FÜR KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus bietet dem Computer Sicherheit vor schädlichen Programmen und wird dadurch selbst zu einem Objekt von Schädlingen, die versuchen können, die Arbeit des Programms zu blockieren oder es sogar vom Computer zu löschen.

Um die Stabilität des Sicherheitssystems für Ihren Computer zu gewährleisten, verfügt Kaspersky Anti-Virus über Mechanismen zum Selbstschutz und zum Schutz vor externem Zugriff.

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus von Kaspersky Anti-Virus nur im Hinblick auf Veränderungen oder Löschen von Dateien auf der Festplatte, sowie von Einträgen in der Systemregistrierung zur Verfügung.

Wenn der Schutz vor Fernsteuerung aktiviert ist, kann es vorkommen, dass gleichzeitig Programme, die der Remote-Administration dienen, eingesetzt werden sollen (z.B. RemoteAdmin). Um die Arbeit mit ihnen zu ermöglichen, werden diese Programme zur Liste der vertrauenswürdigen Programme hinzugefügt und der Parameter **Programmaktivität nicht kontrollieren** wird für sie aktiviert.

➡ Gehen Sie folgendermaßen vor, um die Selbstschutzmechanismen für Kaspersky Anti-Virus zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Selbstschutz** das Kontrollkästchen ☒ **Selbstschutz aktivieren**, damit der Mechanismus zum Schutz von Kaspersky Anti-Virus vor dem Verändern oder Löschen von eigenen Dateien auf der Festplatte, Prozessen im Arbeitsspeicher und Einträgen in der Systemregistrierung wirksam wird.

Aktivieren Sie im Block **Selbstschutz** das Kontrollkästchen ☒ **Option zur externen Steuerung des Systemdiensts deaktivieren**, um alle Versuche zur Fernsteuerung eines Anwendungsdiensts zu blockieren.

Wird versucht, eine der oben genannten Aktionen auszuführen, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).

TECHNOLOGIE ZUR DESINFEKTION EINER AKTIVEN INFEKTION

Moderne Schadprogramme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky Anti-Virus eine schädliche Aktivität im System erkennt, bietet er an, einen speziell dafür vorgesehenen erweiterten Desinfektionsvorgang auszuführen, durch den die Bedrohung neutralisiert und vom Computer gelöscht wird.

Zum Abschluss des Vorgangs erfolgt ein obligatorischer Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.

➡ Gehen Sie folgendermaßen vor, um die Prozedur zur erweiterten Desinfektion zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Kompatibilität** das Kontrollkästchen ☒ **Technologie zur aktiven Desinfektion verwenden**.

ARBEIT VON KASPERSKY ANTI-VIRUS AUF EINEM LAPTOP

Um sparsam mit der Batterie eines Laptops umzugehen, können Sie Untersuchungsaufgaben aufschieben.

Da die Virenuntersuchung und die Aktualisierung relativ viel Ressourcen und Zeit benötigen, empfehlen wir Ihnen, den zeitgesteuerten Start solcher Aufgaben zu deaktivieren. Dadurch können Sie Akkustrom sparen. Bei Bedarf können Sie Kaspersky Anti-Virus auf Befehl aktualisieren oder die Virenuntersuchung manuell starten.

➡ Gehen Sie folgendermaßen vor, um den Dienst zum Stromsparen im Akkubetrieb zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Kompatibilität** das Kontrollkästchen ☒ **Geplante Untersuchungsaufgaben bei Akkubetrieb nicht starten**.

LEISTUNG DES COMPUTERS BEIM AUSFÜHREN VON AUFGABEN

Um die Belastung des Prozessors und der Laufwerkssysteme zu reduzieren, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Das Ausführen von Untersuchungsaufgaben erhöht die Auslastung des Prozessors und der Laufwerkssysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält Kaspersky Anti-Virus beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Arbeit solcher Programme unabhängig sein soll, sollten ihnen keine Systemressourcen überlassen werden.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

➤ *Gehen Sie folgendermaßen vor, damit Untersuchungsaufgaben zurückgestellt werden, wenn sie die Arbeit anderer Programme verlangsamen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Kompatibilität** das Kontrollkästchen ☒ **Ressourcen für andere Programme freigeben**.

FUNKTIONSPARAMETER FÜR KASPERSKY ANTI-VIRUS EXPORTIEREN / IMPORTIEREN

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit, seine Programmeinstellungen zu exportieren und zu importieren.

Diese Option kann beispielsweise von Nutzen sein, wenn Sie Kaspersky Anti-Virus auf Ihrem PC zuhause und im Büro installiert haben. Sie können das Programm zu Hause entsprechend konfigurieren, die Einstellungen auf einer Diskette speichern und mit Hilfe der Importfunktion schnell auf Ihren Computer im Büro laden. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

➤ *Gehen Sie folgendermaßen vor, um die aktuellen Funktionsparameter von Kaspersky Anti-Virus zu exportieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Klicken Sie im Block **Programmeinstellungen verwalten** auf die Schaltfläche **Speichern**.
4. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür aus.

➤ *Gehen Sie folgendermaßen vor, um die Funktionsparameter aus einer Konfigurationsdatei zu importieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Klicken Sie im Block **Programmeinstellungen verwalten** auf die Schaltfläche **Laden**.
4. Wählen Sie im folgenden Fenster eine Datei aus, aus der Sie die Parameter für Kaspersky Anti-Virus importieren möchten.

STANDARDPARAMETER WIEDERHERSTELLEN

Sie können jederzeit zu den empfohlenen Einstellungen für Kaspersky Anti-Virus zurückkehren. Diese gelten als optimal und werden von Kaspersky Lab empfohlen. Die Einstellungen werden durch den Schnellstartassistenten (s. Abschnitt "Schnellstartassistent" auf S. [26](#)) des Programms wiederhergestellt.

Im folgenden Fenster können Sie angeben, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden sollen und für welche Komponenten diese gelten sollen.

Die Liste enthält die Komponenten von Kaspersky Anti-Virus, deren Parameter vom Benutzer verändert wurden. Wenn für eine bestimmte Komponente bei der Arbeit unikale Parameter festgelegt wurden, werden diese ebenfalls in der Liste angegeben.

Diese Listen werden während der Arbeit von Kaspersky Anti-Virus erstellt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Das Erstellen der Listen ist sehr zeitaufwändig. Deshalb wird empfohlen, sie beim Wiederherstellen der ursprünglichen Programmeinstellungen zu speichern.

Nach dem Abschluss des Assistenten wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** eingestellt, wobei die von Ihnen zum Speichern gewählten Parameter berücksichtigt werden. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

➡ *Gehen Sie folgendermaßen vor, um die Schutzeinstellungen wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Einstellungen**.
3. Klicken Sie im Block **Programmeinstellungen verwalten** auf die Schaltfläche **Wiederherstellen**.
4. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Parameter, die gespeichert werden sollen. Klicken Sie auf **Weiter**. Dadurch wird der Konfigurationsassistent gestartet. Folgen Sie den Anweisungen.

BEDROHUNGEN UND AUSNAHMEN

Im Abschnitt **Gefahren und Ausnahmen** des Konfigurationsfensters von Kaspersky Anti-Virus können Sie:

- Kategorie der erkennbaren Bedrohungen auswählen (s. Abschnitt "Kategorien der erkennbaren Bedrohungen auswählen" auf S. [105](#));
- eine vertrauenswürdige Zone für das Programm anlegen.

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die nicht von dem Programm kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz, den Kaspersky Anti-Virus bietet.

Die Vertrauenswürdige Zone wird mit der Liste vertrauenswürdigen Programme (s. Abschnitt "Vertrauenswürdige Programme auswählen" auf S. [105](#)) und mit Ausnahmeregeln (s. Abschnitt "Ausnahmeregeln" auf S. [106](#)) gebildet.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn das Programm den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt / Programm absolut unschädlich ist.

SIEHE AUCH

Kategorien der erkennbaren Bedrohungen auswählen	105
Vertrauenswürdige Programme auswählen.....	105
Regeln für Ausnahmen.....	106
Zulässige Ausschlussmasken für Dateien.....	107
Zulässige Masken für Bedrohungen	108

KATEGORIEN DER ERKENNBAREN BEDROHUNGEN AUSWÄHLEN

Kaspersky Anti-Virus bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Unabhängig von den festgelegten Parametern untersucht und neutralisiert das Programm immer Viren, trojanische Programme und Hackerprogramme. Diese Programme können Ihrem Computer bedeutenden Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrolle für unterschiedliche Arten potentiell gefährlicher Programme.

➡ Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Gefahren und Ausnahmen** aus. Klicken Sie im Block **Bedrohungen** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Bedrohungen** die Bedrohungskategorien, vor denen Sie Ihren Computer schützen möchten.

VERTRAUENSWÜRDIGE PROGRAMME AUSWÄHLEN

Sie können eine Liste mit vertrauenswürdigen Programmen erstellen, deren Datei- und Netzwerkaktivität (einschließlich verdächtiger Aktivität) sowie deren Zugriffe auf die Systemregistrierung nicht kontrolliert werden sollen.

Sie halten beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm Editor verwendet werden, für ungefährlich und deren Untersuchung im Schutz nicht für erforderlich. Das bedeutet, dass Sie diesem Programm vertrauen. Um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen, fügen Sie das Programm Editor zur Liste der vertrauenswürdigen Programme hinzu. Zugleich werden die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms weiterhin auf Viren untersucht. Um ein Programm vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden.

Einige Aktionen, die als gefährlich klassifiziert werden, sind im Rahmen der Funktionalität bestimmter Programme normal. Beispielsweise ist das Abfangen eines Texts, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (Punto Switcher u.ä.) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Durch das Ausschließen vertrauenswürdiger Programme aus der Untersuchung wird es erlaubt, Kompatibilitätsprobleme von Kaspersky Anti-Virus mit anderen Programmen zu lösen (beispielsweise das Problem einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Anti-Virus und durch ein anderes Antiviren-Programm). Außerdem lässt sich auf diese Weise die Leistungsfähigkeit des Computers erhöhen, was insbesondere bei der Verwendung von Serveranwendungen wichtig ist.

Kaspersky Anti-Virus untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr.

➤ Gehen Sie folgendermaßen vor, um ein Programm zur Liste der vertrauenswürdigen Programme hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Gefahren und Ausnahmen** aus.
3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Vertrauenswürdige Programme** auf den Link **Hinzufügen**.
5. Wählen Sie im Kontextmenü ein Programm aus. Bei Auswahl des Punkts **Durchsuchen** wird ein Fenster geöffnet, in dem der Pfad der ausführbaren Datei angegeben werden muss. Bei Auswahl des Punkts **Programme** wird eine Liste der momentan aktiven Programme geöffnet.
6. Legen Sie im folgenden Fenster **Ausnahmen für das Programm** die Parameter der Ausnahmeregel fest.

Mit Hilfe der entsprechenden Links im unteren Bereich der Registerkarte können Sie ein vertrauenswürdiges Programm aus der Liste ändern oder löschen. Um ein Programm aus der Liste auszuschließen, ohne sie zu entfernen, deaktivieren Sie das Kontrollkästchen neben dem Programm.

REGELN FÜR AUSNAHMEN

Ein potentiell gefährliches Programm besitzt keine schädlichen Funktionen, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Virus klassifiziert (not-a-virus). Sie lässt sich beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Internet Security erkannt werden, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme dieser Kategorie von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen.

Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein Programm, das dem Remote-Zugriff dient und die Arbeit auf einem Remote-Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Anti-Virus als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass das Programm gesperrt wird, muss eine Ausnahmeregel für das Programm erstellt werden, die sie entsprechend der Viren-Enzyklopädie als *not-a-virus:RemoteAdmin.Win32.RAdmin.22* erkennt.

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von Kaspersky Anti-Virus untersucht wird.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden.

Ein *Bedrohungstyp* ist ein Status, der einem Objekt bei der Untersuchung von Kaspersky Anti-Virus zugewiesen wird. Der Bedrohungstyp beruht auf der Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die danach einige Programmkomponenten verwenden können (Beispiel Datei-Anti-Virus (s. Abschnitt "Schutz für das Dateisystem des Computers" auf S. 42), Mail-Anti-Virus (s. Abschnitt "E-Mail-Schutz" auf S. 52), Web-Anti-Virus (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. 59)) und ebenso die Aufgaben der Virenuntersuchung.

➤ Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Gefahren und Ausnahmen** aus.

3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf den Link **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Ausnahmeregel** die Parameter der Ausnahmeregel an.

SIEHE AUCH

Zulässige Ausschlussmasken für Dateien	107
Zulässige Masken für Bedrohungen	108

ZULÄSSIGE AUSSCHLUSSMASKEN FÜR DATEIEN

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können. Dazu gehören:

1. Masken ohne Dateipfad:
 - ***.exe** – alle Dateien mit der Endung *exe*;
 - ***.ex?** – alle Dateien mit der Endung *ex?*, wobei anstelle von **?** ein beliebiges Zeichen stehen kann.
 - **test** – alle Dateien mit dem Namen *test*

2. Masken mit absolutem Dateipfad:
 - **C:\dir*.*** oder **C:\dir*** oder **C:\dir** - alle Dateien im Ordner *C:\dir*;
 - **C:\dir*.exe** – alle Dateien mit der Endung *exe* im Ordner *C:\dir*;
 - **C:\dir*.ex?** – alle Dateien mit der Endung *ex?* im Ordner *C:\dir*, wobei anstelle von **?** ein beliebiges Zeichen stehen kann;
 - **C:\dir\test** – nur die Datei *C:\dir\test*.

Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen ☒ **Unterordner einschließen**.

3. Masken mit Dateipfad:
 - **dir*.*** oder **dir*** oder **dir** - alle Dateien in allen Ordnern von *dir*;
 - **dir\test** – alle Dateien mit dem Namen *test* in den Ordnern von *dir*;
 - **dir*.exe** – alle Dateien mit der Endung *exe* in allen Ordnern *dir*;
 - **dir*.ex?** – alle Dateien mit der Endung *ex?* in allen Ordnern von *dir*, wobei anstelle von **?** ein beliebiges Zeichen stehen kann.

Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen ☒ **Unterordner einschließen**.

Die Verwendung der Ausnahmemaske ***.*** oder ***** ist nur zulässig, wenn die auszuschließende Bedrohung gemäß der Viren-Enzyklopädie klassifiziert wird. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Wenn diese Masken ohne Angabe einer Klassifikation verwendet werden, entspricht dies dem Deaktivieren des Schutzes. Außerdem wird davor gewarnt, den Pfad eines virtuellen Laufwerks, das auf Basis eines Dateisystemordners mit dem Befehl `subst` erstellt wurde, oder den Pfad eines Laufwerks, das der Mirror eines Netzwerkordners ist, als Ausnahme auszuwählen. Es kann sein, dass für unterschiedliche Benutzer eines Computers ein identischer Laufwerksname unterschiedliche Ressourcen bezeichnet, was beim Auslösen von Ausnahmeregeln unvermeidlich zu Fehlern führt.

ZULÄSSIGE MASKEN FÜR BEDROHUNGEN

Wenn eine Bedrohung, die ein bestimmtes Verdikt nach der Klassifikation der Viren-Enzyklopädie besitzt, als Ausnahme hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de genannt wird (beispielsweise *not-a-virus:RiskWare.RemoteAdmin.RA.311* oder *Flooder.Win32.Fuxx*).
- den Namen der Bedrohung als Maske, beispielsweise:
 - **not-a-virus*** – Legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
 - ***Riskware.*** – Alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
 - ***RemoteAdmin.*** – Alle Versionen von Programmen zur Fernverwaltung von der Untersuchung ausschließen.

NETZWERK

Im Abschnitt **Netzwerk** des Programmkonfigurationsfensters können Sie die Ports, die von Kaspersky Anti-Virus kontrolliert werden sollen, auswählen und die Untersuchung geschützter Verbindungen anpassen:

- Liste der zu kontrollierenden Ports erstellen.
- Modus zur Untersuchung geschützter Verbindungen (mit dem Protokoll SSL) aktivieren / deaktivieren (s. S. [109](#)).
- Proxyserver-Parameter anpassen (s. S. [112](#)).

SIEHE AUCH

Liste der zu kontrollierenden Ports erstellen.....	108
Untersuchung geschützter Verbindungen	109
Untersuchung geschützter Verbindungen in Mozilla Firefox.....	110
Untersuchung geschützter Verbindungen in Opera.....	111
Proxyserver-Einstellungen.....	112

LISTE DER ZU KONTROLLIERENDEN PORTS ERSTELLEN

Solche Schutzkomponenten wie Mail-Anti-Virus (s. Abschnitt "E-Mail-Schutz" auf S. [52](#)) und Web-Anti-Virus (s. Abschnitt "Schutz für Web-Datenverkehr" auf S. [59](#)) kontrollieren die Datenströme, die durch bestimmte Protokolle übertragen

werden und über bestimmte geöffnete Ports in Ihren Computer eintreffen. Mail-Anti-Virus analysiert beispielsweise die Informationen, die mit dem Protokoll SMTP übertragen werden, Web-Anti-Virus analysiert HTTP-Pakete.

Für die Kontrolle der Ports stehen zwei Modi zur Auswahl:

-  **Alle Netzwerkports kontrollieren.**
-  **Nur ausgewählte Ports überwachen.** Eine Liste der Ports, die gewöhnlich zur Übertragung von E-Mails und HTTP-Datenstrom benutzt werden, gehört zum Lieferumfang des Programms.

➡ *Gehen Sie folgendermaßen vor, um einen Port zur Liste der kontrollierten Ports hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Kontrollierte Ports** auf die Schaltfläche **Auswählen**.
4. Klicken Sie im folgenden Fenster **Netzwerkports** auf den Link **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Netzwerkport** die notwendigen Daten an.

➡ *Gehen Sie folgendermaßen vor, um einen Port aus der Liste der kontrollierten Ports auszuschließen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Kontrollierte Ports** auf die Schaltfläche **Auswählen**.
4. Deaktivieren Sie im folgenden Fenster **Netzwerkports** das Kontrollkästchen ☒ neben der Beschreibung des Ports.

➡ *Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Ports kontrolliert werden sollen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Kontrollierte Ports** auf die Schaltfläche **Auswählen**.
4. Aktivieren Sie im folgenden Fenster **Netzwerkports** das Kontrollkästchen ☒ **Alle Ports für die angegebenen Programme kontrollieren** und klicken Sie im Block unten auf den Link **Hinzufügen**.
5. Wählen Sie im Kontextmenü ein Programm aus. Bei Auswahl des Punkts **Durchsuchen** wird ein Fenster geöffnet, in dem der Pfad der ausführbaren Datei angegeben werden muss. Bei Auswahl des Punkts **Programme** wird eine Liste der momentan aktiven Programme geöffnet.
6. Geben Sie im folgenden Fenster **Programm** eine Beschreibung für das ausgewählte Programm an.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN

Eine Verbindung unter Verwendung des SSL-Protokolls schützt den Datenaustausch. Das SSL-Protokoll erlaubt die Identifikation der am Datenaustausch beteiligten Partner. Dazu dienen elektronische Zertifikate. Außerdem werden die übertragenen Daten verschlüsselt und beim Übertragungsvorgang wird die Datenintegrität gewährleistet.

Diese Besonderheiten des Protokolls werden aber von Angreifern zur Verbreitung schädlicher Programme benutzt, weil die meisten Antiviren-Produkte den SSL-Verkehr nicht untersuchen.

Die Untersuchung von geschützten Verbindungen wird in Kaspersky Anti-Virus realisiert, indem ein Zertifikat von Kaspersky Lab installiert wird. Dieses Zertifikat wird immer verwendet, um die Sicherheit einer Verbindung zu prüfen.

Die Untersuchung des Datenverkehrs nach dem SSL-Protokoll findet künftig mit Hilfe des installierten Kaspersky-Lab-Zertifikats statt. Wenn bei der Verbindung mit einem Server ein inkorrektes Zertifikat gefunden wird (wenn es z.B. von einem Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine Meldung, in der Sie das Zertifikat akzeptieren oder ablehnen, oder Informationen über das Zertifikat anzeigen können. Wenn das Programm im automatischen Modus arbeitet, werden Verbindungen, die ein inkorrektes Zertifikat verwenden, ohne Nachfrage getrennt.

➤ *Gehen Sie folgendermaßen vor, um die Untersuchung geschützter Verbindungen zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen ☒ **Geschützte Verbindungen untersuchen** und klicken Sie auf die Schaltfläche **Zertifikat installieren**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Zertifikat installieren**. Es wird ein Assistent gestartet, der Sie bei der Installation eines Zertifikats unterstützt.

Die automatische Installation eines Zertifikats erfolgt nur bei der Arbeit mit dem Browser Microsoft Internet Explorer. Zur Untersuchung von geschützten Verbindungen in den Browsern Mozilla Firefox und Opera muss das Kaspersky-Lab-Zertifikat manuell installiert werden.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN MOZILLA FIREFOX

Der Browser Mozilla Firefox verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Firefox ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

➤ *Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:*

1. Wählen Sie im Menü des Browsers den Punkt **Extras** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie im Block **Zertifikate** die Registerkarte **Sicherheit** und klicken Sie auf die Schaltfläche **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: %AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.
6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Anzeige von Informationen zu dem Zertifikat dient die Schaltfläche **Ansicht**.

➤ *Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Mozilla Firefox Version 3.x zu installieren:*

1. Wählen Sie im Menü des Browsers den Punkt **Extras** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Klicken Sie auf der Registerkarte **Verschlüsselung** auf die Schaltfläche **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: %AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.
6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Anzeige von Informationen zu dem Zertifikat dient die Schaltfläche **Anzeigen**.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: %AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN OPERA

Der Browser Opera verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Opera ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

➡ Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Extras** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf die Schaltfläche **Zertifikate verwalten**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: %AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.
6. Klicken Sie im folgenden Fenster auf die Schaltfläche **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert. Um Informationen zum Zertifikat anzuzeigen und die Aktionen, bei denen das Zertifikat verwendet werden soll, auszuwählen, wählen Sie das Zertifikat in der Liste aus und klicken Sie auf die Schaltfläche **Anzeigen**.

➡ Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Opera Version 9.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Extras** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf die Schaltfläche **Zertifikate verwalten**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf die Schaltfläche **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: %AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.
6. Klicken Sie im folgenden Fenster auf die Schaltfläche **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: %AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.

PROXYSERVER-EINSTELLUNGEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die entsprechenden Verbindungsparameter anzupassen. Kaspersky Anti-Virus verwendet diese Parameter bei der Arbeit bestimmter Schutzkomponenten und für das Update der Datenbanken und Programm-Module.

Wenn in Ihrem Netzwerk ein Proxyserver verwendet wird, der einen nicht standardmäßigen Port benutzt, ist es erforderlich, diesen Port zur Liste der kontrollierten Ports hinzuzufügen.

➡ *Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Netzwerk**.
3. Klicken Sie im Block **Proxyserver** auf die Schaltfläche **Proxyserver anpassen**.
4. Ändern Sie im folgenden Fenster **Proxyserver-Einstellungen** die Parameter für den Proxyserver.

MELDUNGEN

Bei der Arbeit von Kaspersky Anti-Virus treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit einer bestimmten Komponente festhalten, der dringend behoben werden muss.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Anti-Virus informieren zu lassen, verwenden Sie den Dienst für Benachrichtigungen.

In der Grundeinstellung dienen Popupmeldungen und entsprechende Tonsignale zur Benachrichtigung des Benutzers.

Die Meldungen können durch eine der folgenden Methoden erfolgen:

- Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste
- Tonsignale.
- E-Mail-Nachrichten.

➡ *Gehen Sie folgendermaßen vor, um das Senden von Meldungen zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen**.
3. Deaktivieren Sie das Kontrollkästchen ☐ **Über Ereignisse benachrichtigen**.

Auch wenn das Senden von Meldungen deaktiviert wurde, werden Informationen über Ereignisse, die bei der Arbeit von Kaspersky Anti-Virus eintreten, im Bericht über die Programmarbeit aufgezeichnet.

➡ *Gehen Sie folgendermaßen vor, um eine Methode für das Senden von Meldungen auszuwählen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen** und klicken Sie auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster **Meldungen** eine Methode für das Senden von Meldungen aus.

SIEHE AUCH

Audiosignale zur Begleitung von Benachrichtigungen deaktivieren	113
E-Mail-Benachrichtigungen senden.....	113

AUDIOSIGNALE ZUR BEGLEITUNG VON BENACHRICHTIGUNGEN DEAKTIVIEREN

In der Grundeinstellung werden alle Meldungen von einem Audiosignal begleitet. Dazu wird das Soundschema von Microsoft Windows verwendet. Das Kontrollkästchen ☒ **Standardsoundschema Windows Default verwenden** erlaubt es, das verwendete Schema zu ändern. Wenn das Kontrollkästchen deaktiviert ist, wird das Soundschema der vorhergehenden Programmversion verwendet.

➔ *Gehen Sie folgendermaßen vor, um die Audiosignale zur Begleitung von Benachrichtigungen zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen**.
3. Deaktivieren Sie das Kontrollkästchen ☒ **Audiosignale für Meldungen aktivieren**.

E-MAIL-BENACHRICHTIGUNGEN SENDEN

Für das Senden von E-Mail-Benachrichtigungen ist es erforderlich, die E-Mail-Parameter anzupassen.

➔ *Gehen Sie folgendermaßen vor, um die E-Mail-Parameter für das Senden von Meldungen anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Meldungen**.
3. Aktivieren das Kontrollkästchen ☒ **E-Mails über Ereignisse senden** und klicken Sie auf die Schaltfläche **E-Mail-Einstellungen**.
4. Geben Sie im folgenden Fenster **E-Mail-Meldungen anpassen** die Versandparameter an.

BERICHTE UND SPEICHER

Dieser Abschnitt enthält Parameter, die die Arbeit mit der Datenverwaltung von Kaspersky Anti-Virus regulieren.

Die *Datenverwaltung der Anwendung* umfasst Objekte, die während der Arbeit von Kaspersky Anti-Virus in der Quarantäne und im Backup gespeichert wurden, sowie Dateien der Berichte über die Arbeit der Programmkomponenten.

In diesem Abschnitt können Sie:

- Einstellungen für die Erstellung (s. S. [114](#)) und Speicherung von Berichten (s. S. [114](#)) konfigurieren;
- Einstellungen für Quarantäne und Backup (s. S. [116](#)) konfigurieren.

SIEHE AUCH

Einträge über Ereignisse zum Bericht hinzufügen	114
Berichte leeren	114
Berichte speichern	114
Quarantäne für möglicherweise infizierte Objekte	115
Sicherungskopien gefährlicher Objekte	116
Arbeit mit Objekten in der Quarantäne	116
Quarantäne- und Backup-Objekte speichern	116
Berichte	126

EINTRÄGE ÜBER EREIGNISSE ZUM BERICHT HINZUFÜGEN

Sie können festlegen, dass dem Schutzbericht auch Einträge über unkritische Ereignisse sowie Ereignisse, die die Registrierung und das Dateisystem betreffen, hinzugefügt werden. In der Grundeinstellung werden diese Einträge nicht zum Bericht hinzugefügt.

➤ *Gehen Sie folgendermaßen vor, damit dem Schutzbericht auch Einträge über unkritische Ereignisse sowie über Ereignisse der Registrierung und / oder des Dateisystems hinzugefügt werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher** aus.
3. Aktivieren Sie im Block **Berichte** das entsprechende Kontrollkästchen ☒.

BERICHTE LEEREN

Informationen über die Arbeit von Kaspersky Anti-Virus werden in den Berichten aufgezeichnet. Diese können bereinigt werden.

➤ *Um die Berichte zu leeren, machen Sie Folgendes:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher**.
3. Klicken Sie im Block **Berichte** auf die Schaltfläche **Leeren**.
4. Aktivieren Sie im folgenden Fenster **Informationen aus Berichten löschen** die Kontrollkästchen der Berichtskategorien, die Sie bereinigen möchten.

BERICHTE SPEICHERN

Sie können die maximale Speicherdauer für Ereignisberichte festlegen (Kontrollkästchen ☒ **Berichte speichern für maximal**). Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Die maximale Speicherdauer kann geändert oder völlig aufgehoben werden. Außerdem kann die Größe einer Berichtsdatei beschränkt werden (Kontrollkästchen ☒ **Maximale Dateigröße**). Die maximale Größe beträgt

standardmäßig 1024 MB. Wenn die maximale Größe erreicht wird, wird der Inhalt der Datei mit neuen Einträgen überschrieben. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

➡ Gehen Sie folgendermaßen vor, um die Parameter für das Speichern von Berichten anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher** aus.
3. Aktivieren Sie im folgenden Fenster im Block **Berichte** die entsprechenden Kontrollkästchen ☒ und ändern Sie, falls erforderlich, die maximale Berichtsgröße und die Speicherdauer.

QUARANTÄNE FÜR MÖGLICHERWEISE INFIZIERTE OBJEKTE

Die *Quarantäne* ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig werden, von Viren oder Virenmodifikationen infiziert zu sein.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus, Mail-Anti-Virus und Proaktiver Schutz gefunden und in die Quarantäne verschoben werden.

Objekte werden aufgrund der Arbeit von Datei-Anti-Virus und Mail-Anti-Virus sowie während der Virensuche in die Quarantäne verschoben, wenn:

- *Der Code des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert.*

Die Datenbanken von Kaspersky Anti-Virus enthalten jene Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Signaturen aufgenommen wurden, klassifiziert Kaspersky Anti-Virus das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- *Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Bedrohungssignaturen enthalten jedoch keine entsprechenden Einträge.*

Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb klassifiziert Kaspersky Anti-Virus dieses Objekt als möglicherweise infiziertes Objekt.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem *heuristischen Code Analysator* ermittelt, mit dessen Hilfe bis zu 92 % neuer Viren erkannt werden. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Was den Proaktiven Schutz betrifft, so wird ein Objekt von der Komponente in die Quarantäne verschoben, wenn aufgrund der Analyse seines Verhaltens die Reihenfolge der Aktionen, die das Objekt ausführt, als verdächtig eingestuft wird.

Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Möglicherweise kann die Bedrohung von Kaspersky Anti-Virus eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken des Programms aktualisiert wurden. Deshalb untersucht das Programm die Quarantäneobjekte nach jedem Update (s. S. [90](#)).

SICHERUNGSKOPIEN GEFÄHRLICHER OBJEKTE

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine *Sicherungskopie* ist eine Kopie des gefährlichen Originalobjekts. Sie wird bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert.

Das *Backup* ist ein spezieller Speicher für Sicherungskopien gefährlicher Objekte, die verarbeitet oder gelöscht werden. Die wichtigste Funktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

ARBEIT MIT OBJEKTEN IN DER QUARANTÄNE

Mit Objekten, die in die Quarantäne verschoben wurden, können Sie folgende Aktionen ausführen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Alle möglicherweise infizierten Quarantäneobjekte unter Verwendung der aktuellen Version der Datenbanken von Kaspersky Anti-Virus untersuchen und desinfizieren.
- Dateien wiederherstellen entweder in einem vom Benutzer gewählten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden.
- Ein beliebiges Quarantäneobjekt oder eine Gruppe ausgewählter Objekte löschen.
- Quarantäneobjekte zur Untersuchung an Kaspersky Lab schicken.

➡ *Gehen Sie folgendermaßen vor, um mit Quarantäneobjekten zu arbeiten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Quarantäne**.
2. Führen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** die entsprechenden Aktionen aus.

QUARANTÄNE- UND BACKUP-OBJEKTE SPEICHERN

Sie können folgende Parameter für Quarantäne und Backup anpassen:

- Legen Sie eine maximale Speicherdauer für Objekte in der Quarantäne und Sicherungskopien im Backup fest (Kontrollkästchen ☒ **Objekte speichern für maximal**). Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer ändern oder diese Beschränkung völlig aufheben.
- Eine maximale Größe für den Datenspeicher festlegen (Kontrollkästchen ☒ **Maximale Größe**). Die maximale Größe beträgt standardmäßig 100 MB. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

➡ *Gehen Sie folgendermaßen vor, um die Parameter für die Quarantäne und das Backup anzupassen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Berichte und Speicher** aus.
3. Aktivieren Sie im Block **Quarantäne und Backup** die entsprechenden Kontrollkästchen und legen Sie bei Bedarf eine maximale Größe für den Datenspeicher fest.

FEEDBACK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um das Sammeln statistischer Daten über die Typen und Quellen neuer Bedrohungen zu beschleunigen und die Entwicklung entsprechender Neutralisierungsmethoden zu optimieren, bietet Kaspersky Lab Ihnen die Teilnahme an dem Dienst *Kaspersky Security Network* an.

Die Verwendung von Kaspersky Security Network sieht vor, dass bestimmte Informationen an Kaspersky Lab gesendet werden. Es werden folgende Daten gesendet:

- Individuelle ID, die Ihrem Computer vom Kaspersky Lab-Produkt zugewiesen wird. Dieser Identifikator charakterisiert die Hardwareparameter Ihres Computers und enthält keinerlei persönliche Informationen.
- Informationen über die Bedrohungen, die von den Programmkomponenten gefunden wurden. Die Auswahl der Informationen ist vom Typ der gefundenen Bedrohung abhängig.
- Informationen über das System: Version des Betriebssystems, installierte Service Packs, geladene Dienste und Treiber, Versionen von Browsern und Mailprogrammen, Erweiterungen für Browser, Versionsnummer des installierten Kaspersky-Lab-Programms.

➡ *Gehen Sie folgendermaßen vor, um das Senden einer Statistik an Kaspersky Security Network zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Feedback** aus.
3. Aktivieren Sie das Kontrollkästchen ☒ **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

AUSSEHEN DES PROGRAMMS

Sie können das Aussehen von Kaspersky Anti-Virus verändern, indem Sie unterschiedliche grafische Elemente und Farbschemen erstellen und verwenden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen (Programmsymbol im Infobereich der Microsoft Windows-Taskleiste und Popupmeldungen).

SIEHE AUCH

Aktive Elemente der Benutzeroberfläche	117
Grafische Oberfläche von Kaspersky Anti-Virus.....	118

AKTIVE ELEMENTE DER BENUTZEROBERFLÄCHE

Um die aktiven Elemente der Benutzeroberfläche anzupassen (z.B. Symbol von Kaspersky Anti-Virus in der Taskleiste und Popupmeldungen), stehen folgende Möglichkeiten zur Verfügung:

Animation des Symbols bei Aufgabenausführung verwenden.

In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Symbol im Infobereich. Wird beispielsweise die Untersuchung eines Skripts ausgeführt, dann erscheint im Hintergrund des Symbols ein kleines Piktogramm mit einem Skript. Bei der Untersuchung einer E-Mail-Nachricht erscheint das Piktogramm eines Briefs. Das Symbol von Kaspersky Anti-Virus ist animiert. Es gibt in diesem Fall nur den Schutzstatus Ihres Computers wieder: Wenn der Schutz aktiviert ist, ist das Symbol farbig. Wenn der Schutz angehalten oder ausgeschaltet wurde, ist es grau.

Transparenz für Meldungsfenster verwenden.

Alle Operationen des Programms, die Ihre sofortige Aufmerksamkeit oder Entscheidung erfordern, besitzen das Aussehen einer Popupmeldung die über dem Programmsymbol im Infobereich erscheinen. Die Meldungsfenster sind halbtransparent, damit sie Ihre Arbeit nicht stören. Wenn der Mauscursor auf das Meldungsfenster geführt wird, wird die Transparenz aufgehoben.

Über Neuigkeiten benachrichtigen.

Standardmäßig erscheint beim Eintreffen von Nachrichten in der Taskleiste ein spezielles Symbol. Durch Klick auf das Symbol wird ein Fenster mit dem Nachrichtentext geöffnet.

"Protected by Kaspersky Lab" über dem Microsoft Windows-Begrüßungsbildschirm anzeigen.

Dieser Indikator erscheint in der Grundeinstellung rechts oben am Bildschirmrand, wenn Kaspersky Anti-Virus gestartet wird. Er informiert darüber, dass der Schutz Ihres Computers vor jeder Art von Bedrohung aktiviert ist.

Wenn der Computer, auf dem das Programm installiert ist, ein Betriebssystem der Produktfamilie Microsoft Windows Vista verwendet, steht diese Option nicht zur Verfügung.

➡ Gehen Sie folgendermaßen vor, um die aktiven Elemente der Benutzeroberfläche anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Ansicht**.
3. Aktivieren oder deaktivieren Sie im Block **Symbol in der Taskleiste** die entsprechenden Kontrollkästchen .

GRAFISCHE OBERFLÄCHE VON KASPERSKY ANTI-VIRUS

Alle auf der Oberfläche von Kaspersky Anti-Virus verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren.

➡ Gehen Sie folgendermaßen vor, um eine andere grafische Oberfläche zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster den Abschnitt **Ansicht**.
3. Aktivieren Sie im Block **Grafische Oberflächen** das Kontrollkästchen  **Alternative Programmoberfläche verwenden**, um eine grafische Oberfläche einzubinden. Geben Sie im Eingabefeld den Ordner mit den Parametern der grafischen Oberfläche an. Klicken Sie zur Auswahl eines Ordners auf die Schaltfläche **Durchsuchen**.

PROFILE FÜR KASPERSKY ANTI-VIRUS VERWENDEN

Wenn bestimmte Programme (z.B. Spiele) im Vollbildmodus verwendet werden, kann es erforderlich sein, einzelne Funktionen von Kaspersky Anti-Virus (insbesondere den Benachrichtigungsdienst) zu deaktivieren. Solche Programme sind oft sehr ressourcenaufwändig und deshalb könnte die gleichzeitige Ausführung bestimmter Aufgaben von Kaspersky Anti-Virus zur Verlangsamung ihrer Arbeit führen.

Damit der Benutzer nicht jedes Mal, wenn er Vollbild-Anwendungen einsetzt, manuell die Benachrichtigungen ausschalten und Aufgaben anhalten muss, bietet Kaspersky Anti-Virus die Möglichkeit, diese Parameter mit Hilfe eines Profils für Spiele vorübergehend zu ändern. Das Profil für Spiele erlaubt es, beim Wechsel in den Vollbildmodus gleichzeitig die Parameter aller Komponenten zu ändern und beim Verlassen des Vollbildmodus die vorgenommenen Änderungen wieder rückgängig zu machen.

Die Ereignisbenachrichtigungen werden beim Wechsel in den Vollbildmodus automatisch deaktiviert. Außerdem können folgende Parameter angegeben werden:

- ☒ **Aktion automatisch auswählen.** Bei Auswahl dieser Variante wird als Reaktion für alle Komponenten die automatische Auswahl einer Aktion verwendet, selbst wenn in ihren Einstellungen die Variante  **Aktion erfragen** festgelegt wurde. Auf diese Weise wird der Benutzer beim Fund von Bedrohungen nicht nach einer Aktion gefragt, sondern das Programm wählt automatisch eine Aktion aus.
- ☒ **Update nicht ausführen** und ☒ **Geplante Untersuchungsaufgaben nicht starten.** Es wird empfohlen, diese Parameter zu verwenden, um eine Verlangsamung von Vollbild-Anwendungen zu vermeiden.

➡ *Gehen Sie folgendermaßen vor, um die Verwendung des Profils für Spiele zu aktivieren:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Profil für Spiele**.
3. Aktivieren Sie das Kontrollkästchen ☒ **Profil für Spiele aktivieren** und geben Sie die entsprechenden Parameter an.

ZUSÄTZLICHE OPTIONEN

Es ist eine schwierige Aufgabe, die Sicherheit eines Computers zu gewährleisten. Dafür sind Kenntnisse über Besonderheiten der Funktion eines Betriebssystems und über potentielle Schwachstellen erforderlich. Zudem erschweren die große Menge und die Vielfalt der Informationen über die Systemsicherheit deren Analyse und Verarbeitung.

Um spezifische Aufgaben, die die Sicherheit des Computers gewährleisten, zu vereinfachen, verfügt Kaspersky Anti-Virus über unterschiedliche Assistenten und Werkzeuge.

- Virtuelle Tastatur (s. S. [120](#)), sodass keine über die Tastatur eingegebenen Daten erfasst werden können.
- Der Assistent zum Erstellen einer Notfall-CD (s. S. [121](#)) dient dazu, die Funktionsfähigkeit des Systems nach einem Virenangriff wiederherzustellen, wenn Systemdateien des Betriebssystems beschädigt wurden und der Computer nicht mehr hochgefahren werden kann.
- Der Assistent zur Browser-Konfiguration (s. S. [123](#)) führt eine Analyse der Einstellungen des Browsers Microsoft Internet Explorer aus. Dabei werden die Einstellungen hauptsächlich im Hinblick auf die Sicherheit bewertet.
- Der Assistent zur Wiederherstellung nach einer Infektion (s. S. [124](#)) beseitigt im System die Spuren von schädlichen Objekten.
- Der Assistent zum Löschen von Aktivitätsspuren (s. S. [125](#)) sucht und beseitigt im System die Aktivitätsspuren des Benutzers.

IN DIESEM ABSCHNITT

Virtuelle Tastatur	120
Notfall-CD	121
Browser-Konfiguration	123
Wiederherstellung nach Infektion	124
Assistent zum Löschen von Aktivitätsspuren	125

VIRTUELLE TASTATUR

Bei der Arbeit auf einem Computer ist es häufig erforderlich, persönliche Daten, Benutzername und Kennwort einzugeben. Beispiele sind die Anmeldung auf Internetseiten, der Besuch von Online-Shops usw.

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mit Hilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

Die virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

Die virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, weil die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.

Viele Spyware-Programme besitzen Funktionen zum Anlegen von Screenshots, die an Angreifer für Analyse und Sammeln von persönlichen Benutzerdaten automatisch übergeben werden. Die virtuelle Tastatur schützt die eingegebenen persönlichen Daten, die durch das Anlegen von Screenshots abgefangen werden können..

Die virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie mit den Internetbrowsern Microsoft Internet Explorer und Mozilla Firefox arbeiten.

➡ Gehen Sie folgendermaßen vor, um die virtuelle Tastatur zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Virtuelle Tastatur**.
3. Geben Sie die erforderlichen Daten über die virtuelle Tastatur ein. Vergewissern Sie sich, dass die Daten im erforderlichen Feld eingegeben wurden. Die Funktionstasten (**Umschalt**, **Alt**, **Strg**) der virtuellen Tastatur verfügen über eine Einrastfunktion (wenn beispielsweise die **Umschalt**-Taste einmal angeklickt wurde, werden alle Zeichen groß geschrieben). Um die Einrastfunktion aufzuheben, klicken Sie erneut auf die Funktionstaste.

NOTFALL-CD

Kaspersky Anti-Virus enthält einen Dienst zum Erstellen einer Notfall-CD.

Die Notfall-CD dient zur Untersuchung und Desinfektion infizierter x86-kompatibler Computer. Sie kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools (z.B. Kaspersky AVPTool) möglich ist, die unter dem Betriebssystem gestartet werden. Dabei wird die Effektivität der Desinfektion gesteigert, weil die im System vorhandenen Schädlinge nicht die Kontrolle übernehmen können, während das Betriebssystem hochgefahren wird.

Eine Notfall-CD wird auf Basis eines Linux-Betriebssystemkerns erstellt und ist eine ISO-Datei, die folgende Elemente umfasst:

- System- und Konfigurationsdateien für Linux.
- eine Auswahl von Tools zur Betriebssystemdiagnose
- Auswahl von sonstigen Utilities (Datei-Manager u.a.).
- Dateien für Kaspersky Rescue Disk.
- Dateien, die die Antiviren-Datenbanken enthalten.

Ein Computer, dessen Betriebssystem beschädigt ist, wird über das CD / DVD-ROM-Laufwerk hochgefahren. Dafür muss auf dem Computer ein entsprechendes Gerät installiert sein.

➡ Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+**.
3. Klicken Sie auf die Schaltfläche **Notfall-CD**, um den Assistenten für die Notfall-CD zu starten.
4. Folgen Sie den Anweisungen des Assistenten.
5. Verwenden Sie die Datei, die mit Hilfe des Assistenten erstellt wurde, um eine Bootdisk (CD/DVD) zu brennen. Dafür kann ein Brennprogramm für CDs / DVDs (z.B. Nero) eingesetzt werden.

SIEHE AUCH

Notfall-CD erstellen	122
Hochfahren eines Computers mit Hilfe der Notfall-CD	122

NOTFALL-CD ERSTELLEN

Das Anlegen einer Notfall-CD umfasst das Erstellen eines Disk-Abbild (ISO-Datei) mit den aktuellen Programm-Datenbanken und Konfigurationsdateien.

Ein Original des Disk-Abbilds, auf dessen Basis eine neue Datei erstellt wird, kann von einem Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Die Abbild-Datei, die vom Assistenten erstellt wurde, wird unter dem Namen *rescuecd.iso* im Ordner "Dokumente und Einstellungen\All Users\Anwendungsdaten\Kaspersky Lab\AVP9\Data\Rdisk" ("ProgramData\Kaspersky Lab\AVP9\Data\Rdisk" – für Microsoft Vista) abgelegt. Wenn der Assistent im angegebenen Ordner eine früher erstellte Abbild-Datei gefunden hat, aktivieren Sie das Kontrollkästchen ☒ **Vorhandenes Abbild verwenden**. Sie können die Datei als Basis für das Disk-Abbild verwenden und sofort mit Schritt 3 (Abbild aktualisieren) fortfahren. Wenn der Assistent keine Abbild-Datei gefunden hat, fehlt dieses Kontrollkästchen.

Die Notfall-CD wird mit Hilfe eines Assistenten erstellt, der aus einer Reihe von Fenstern (Schritten) besteht. Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

SIEHE AUCH

Notfall-CD	121
Hochfahren eines Computers mit Hilfe der Notfall-CD	122

HOCHFAHREN EINES COMPUTERS MIT HILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem hochzufahren, ist eine Abbild-Datei (.iso) der Notfall-CD erforderlich. Sie können die Datei von einem Kaspersky-Lab-Server herunterladen oder eine vorhandene Datei aktualisieren.

Im Folgenden wird die Arbeit der Notfall-CD ausführlich erläutert. Während des Downloads der Datei finden folgende Operationen statt:

1. Die Hardware des Computers wird automatisch ermittelt.
2. Auf den Festplatten wird nach Dateisystemen gesucht. Gefundene Dateisysteme erhalten einen Namen, der mit C beginnt.

Die Namen, die den Festplatten und Wechselmedien zugewiesen werden, können von ihren Namen im Betriebssystem abweichen.

Wenn sich das Betriebssystem des Computers, der hochgefahren werden soll, im Ruhezustand befindet oder das Dateisystem den Status *unclean* besitzt, weil beim Herunterfahren ein Fehler aufgetreten ist, können Sie entscheiden, ob das Dateisystem gemountet oder der Computer neu gestartet werden soll.

Das Mounten des Dateisystems kann zu seiner Beschädigung führen.

3. Die Auslagerungsdatei von Microsoft Windows *pagefile.sys* wird gesucht. Wenn sie nicht vorhanden ist, wird die Größe des virtuellen Speichers durch die Größe des Arbeitsspeichers begrenzt.
4. Eine Sprache wird ausgewählt. Wenn innerhalb einer bestimmten Zeit keine Auswahl stattfindet, wird standardmäßig die Sprache Englisch gewählt.
5. Es werden Ordner zum Speichern von Antiviren-Datenbanken, Berichten, Quarantäne und sonstigen Dateien gesucht (erstellt). In der Grundeinstellung werden die Ordner des Kaspersky-Lab-Programms verwendet, das auf dem infizierten Computer installiert ist (*ProgramData/Kaspersky Lab/AVP9* – für Microsoft Windows Vista, *Dokumente und Einstellungen/All Users/Anwendungsdaten/Kaspersky Lab/AVP9* – für ältere Versionen von Microsoft Windows). Wenn diese Ordner des Programms nicht gefunden werden, wird versucht, sie zu erstellen. Falls die Ordner nicht gefunden wurden und nicht erstellt werden können, wird auf einem der Laufwerke der Ordner *kl.files* erstellt.
6. Es wird versucht, mit Hilfe der Daten, die in den Systemdateien des hochzufahrenden Computers gefunden werden, die Netzwerkverbindungen anzupassen.
7. Das grafische Subsystem wird geladen und Kaspersky Rescue Disk wird gestartet.

Im Rettungsmodus sind nur die Aufgaben zur Virensuche und zum Update der Datenbanken aus einer lokalen Quelle verfügbar, sowie das Rollback für Updates und die Anzeige der Statistik.

➡ Gehen Sie folgendermaßen vor, um das Betriebssystem des infizierten Computers hochzufahren:

1. Wählen Sie in den BIOS-Einstellungen das Booten von CD/DVD-ROM (weitere Informationen können der Dokumentation zum Motherboard Ihres Computers entnommen werden).
2. Legen Sie die Disk, auf die das Disk-Abbild gebrannt wurde, in das CD/DVD-Laufwerk des infizierten Computers ein.
3. Starten Sie den Computer neu.

Danach wird der Computer nach dem oben beschriebenen Algorithmus hochgefahren. Ausführliche Informationen über die Funktionen der Notfall-CD gibt die Hilfe zu Kaspersky Rescue Disk.

SIEHE AUCH

Notfall-CD	121
Notfall-CD erstellen	122

BROWSER-KONFIGURATION

Der Assistent zur Browser-Konfiguration führt eine Analyse der Einstellungen des Browsers Microsoft Internet Explorer aus. Dabei werden die Einstellungen vorrangig im Hinblick auf die Sicherheit bewertet, weil bestimmte benutzerdefinierte oder standardmäßige Parameter zu Sicherheitsproblemen führen können.

Der Assistent prüft, ob die aktuellen Updates für den Browser installiert sind und ob seine Einstellungen potentielle Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können, um Ihrem Computer zu beschädigen. Beispiele für zu untersuchenden Objekte:

- **Cache des Microsoft Internet Explorer.** Der Zwischenspeicher enthält vertrauliche Daten und kann außerdem Aufschluss darüber geben, welche Ressourcen der Benutzer besucht hat. Viele schädliche Objekte lesen beim Scannen der Festplatte auch den Zwischenspeicher. Auf diese Weise können Angreifer die Mailadressen von Benutzern erhalten. Es wird empfohlen, den Zwischenspeicher zu leeren, wenn die Arbeit mit dem Browser beendet wird.

- **Anzeige von Erweiterungen für das System bekannte Dateitypen.** Für Benutzer ist es vorteilhaft, die tatsächliche Dateierweiterung zu sehen. Viele schädliche Objekte verwenden eine doppelte Erweiterung. In diesem Fall sieht der Benutzer nur einen Teil des Dateinamens, nicht aber die tatsächliche Erweiterung. Diese Methode wird häufig von Angreifern benutzt. Es wird empfohlen, die Anzeige von Erweiterungen für Dateien bekannter Formate zu aktivieren.
- **Liste mit vertrauenswürdigen Seiten.** Schädliche Objekte können einer solchen Liste Links zu Seiten, die von Angreifern erstellt wurden, hinzufügen.

Schließen Sie alle Browserfenster von Microsoft Internet Explorer, bevor mit der Diagnose begonnen wird.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob in den Einstellungen des Browsers Sicherheitsprobleme vorliegen, die sofort behoben werden müssen. Das Ergebnis der Untersuchung besteht in einer Liste von Aktionen, die ausgeführt werden sollten, um die Probleme zu beheben. Die Aktionen sind nach der Priorität der gefundenen Probleme in Kategorien angeordnet.

Beim Abschluss des Assistenten wird ein Bericht erstellt, der zur Analyse an Kaspersky Lab geschickt werden kann.

Es sollte berücksichtigt werden, dass bestimmte Einstellungen zu Problemen bei der Anzeige spezieller Seiten führen können (beispielsweise wenn sie ActiveX-Elemente verwenden). Das Problem lässt sich lösen, indem solche Seiten in die vertrauenswürdige Zone aufgenommen werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

➡ Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Browser-Konfiguration**.

WIEDERHERSTELLUNG NACH INFEKTION

Der Assistent zur Wiederherstellung nach einer Infektion beseitigt im System die Spuren von schädlichen Objekten. Die Kaspersky-Lab-Spezialisten empfehlen, den Assistenten nach der Desinfektion des Computers zu starten, um sicherzustellen, dass alle Bedrohungen und die von ihnen verursachten Beschädigungen beseitigt werden. Der Assistent kann auch verwendet werden, wenn der Verdacht auf eine Infektion eines Computers besteht.

Der Assistent prüft, ob im System Veränderungen vorliegen. Dazu zählen z.B.: blockierter Zugriff auf die Netzwerkumgebung, veränderte Dateierweiterungen bekannter Formate, blockierte Systemsteuerung usw. Mögliche Gründe für das Auftreten solcher Beschädigungen sind die Aktivität schädlicher Programme, Systemabstürze sowie die Verwendung inkorrekt funktionierender Systemoptimierungsprogramme.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob im System Beschädigungen vorliegen, die sofort behoben werden müssen. Das Ergebnis der Untersuchung besteht in einer Liste von Aktionen, die ausgeführt werden sollten, um die Beschädigungen zu beheben. Die Aktionen sind nach der Priorität der gefundenen Probleme in Kategorien angeordnet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

➡ Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Wiederherstellung nach Infektion**.

ASSISTENT ZUM LÖSCHEN VON AKTIVITÄTSSPUREN

Während der Arbeit auf dem Computer werden die Aktionen des Benutzers im System registriert. Dabei werden folgende Daten gespeichert:

- Verlauf mit Informationen über:
 - besuchte Webseiten.
 - den Start von Programmen
 - Suchanfragen.
 - das Öffnen / Speichern von Dateien mit bestimmten Anwendungen.
- Einträge im Systembericht von Microsoft Windows
- temporäre Dateien u.a.

Alle genannten Informationsquellen über die Benutzeraktivität können sensible Daten wie z.B. Kennwörter enthalten und von Angreifern analysiert werden. Allerdings verfügt der Benutzer häufig nicht über ausreichende Kenntnisse, um dieser Methode des Diebstahls wertvoller Informationen vorzubeugen.

Kaspersky Anti-Virus verfügt über einen Assistenten zum **Löschen von Aktivitätsspuren**. Dieser Assistent führt im System die Suche nach Spuren von Benutzeraktivität und den Betriebssystemparametern, die zum Sammeln von Informationen über die Aktivität dienen, durch.

Es werden laufend Informationen über die Aktivität des Benutzers im System gesammelt. Der Start einer beliebigen Datei oder das Öffnen eines Dokuments werden in einem Verlauf festgehalten, und das Systemjournal von Microsoft Windows registriert eine Vielzahl von Ereignissen, die im System vorkommen. Deshalb kann es sein, dass bei einem wiederholten Start des Assistenten zum **Löschen von Aktivitätsspuren** gefunden werden, die beim vorhergehenden Start des Assistenten bereits gelöscht worden sind. Bestimmte Dateien wie z.B. eine Journaldatei von Microsoft Windows können vom System verwendet werden, während sie vom Assistenten gelöscht werden sollen. Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten. Im Verlauf eines Neustarts können solche Dateien aber erneut erstellt werden, was dazu führt, dass sie wieder als Aktivitätsspuren erkannt werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

➡ *Gehen Sie folgendermaßen vor, den Assistenten zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Sicherheit+** und klicken Sie auf die Schaltfläche **Löschen von Aktivitätsspuren**.

BERICHTE

Die Arbeit jeder Komponente von Kaspersky Anti-Virus und die Ausführung jeder Untersuchungs- und Updateaufgabe werden in einem Bericht protokolliert.

Bei der Arbeit mit Berichten können Sie folgende Aktionen ausführen:

- Komponente / Aufgabe auswählen (s. S. [126](#)), für die ein Ereignisbericht angezeigt werden soll.
- Datengruppierungen verwalten (s. S. [127](#)) und deren Bildschirmanzeige (s. S. [129](#)).
- Zeitplan erstellen (s. S. [127](#)), nach dem Kaspersky Anti-Virus Sie über die Bereitschaft eines Berichts benachrichtigen soll.
- auswählen, für welchen Ereignistyp (s. S. [128](#)) ein Bericht erstellt werden soll.
- auswählen, in welcher Form die statistischen Informationen auf dem Bildschirm dargestellt werden sollen - als Tabelle oder Grafik (s. S. [130](#)).
- Bericht in einer Datei speichern (s. S. [130](#)).
- komplexe Filterbedingungen (s. S. [130](#)) festlegen.
- Suche nach Ereignissen (s. S. [131](#)) organisieren, die im System eingetreten und vom Programm verarbeitet wurden.

IN DIESEM ABSCHNITT

Komponente oder Aufgabe für das Erstellen eines Berichts auswählen	126
Anordnung von Informationen im Bericht	127
Über Bereitschaft des Berichts benachrichtigen	127
Ereignistyp auswählen.....	128
Darstellung von Daten auf dem Bildschirm.....	129
Erweiterte Statistikanzeige	130
Bericht in Datei speichern.....	130
Verwendung der komplexen Filterung.....	130
Suche nach Ereignissen.....	131

KOMPONENTE ODER AUFGABE FÜR DAS ERSTELLEN EINES BERICHTS AUSWÄHLEN

Sie können Informationen über die Ereignisse erhalten, die bei der Arbeit der einzelnen Komponenten von Kaspersky Anti-Virus oder bei der Ausführung von Aufgaben (z.B. Datei-Anti-Virus, Update usw.) eingetreten sind.

➤ Gehen Sie folgendermaßen vor, um einen Bericht über eine bestimmte Komponente oder Aufgabe zu erhalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster links in der Dropdown-Liste eine Komponente oder eine Aufgabe aus, für die ein Bericht erstellt werden soll. Bei Auswahl des Punkts **Schutz-Center** wird ein Bericht für alle Schutzkomponenten erstellt.

ANORDNUNG VON INFORMATIONEN IM BERICHT

Sie können die Anordnung der im Bericht enthaltenen Daten steuern. Die Informationen können nach unterschiedlichen Merkmalen sortiert werden. Die Auswahl der Merkmale ist für jede Komponente und Aufgaben individuell. Folgende Varianten stehen zur Auswahl:

- **Unsortiert.** Alle Ereignisse werden angezeigt.
- **Nach Aufgabe anordnen.** Die Daten werden nach den Aufgaben, die von den Komponenten von Kaspersky Anti-Virus ausgeführt wurden, angeordnet.
- **Nach Programmen anordnen.** Die Daten werden nach Programmen angeordnet, die im System aktiv waren und von Kaspersky Anti-Virus verarbeitet wurden.
- **Nach Untersuchungsergebnis anordnen.** Die Daten werden nach den Ergebnissen der Untersuchung oder Verarbeitung eines Objekts angeordnet.



Abbildung 13. Anordnungsmerkmale für Informationen im Bericht

Zur Vereinfachung und Verkleinerung der Gruppierung ist eine Suche (s. Abschnitt "Suche nach Ereignissen" auf S. [131](#)) nach einem Schlüsselwort vorgesehen. Außerdem können Sie die Suchkriterien festlegen.

➤ Gehen Sie folgendermaßen vor, um die Anordnung nach einem bestimmten Merkmal zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster in der Dropdown-Liste ein Anordnungsmerkmal aus.

ÜBER BEREITSCHAFT DES BERICHTS BENACHRICHTIGEN

Sie können einen Zeitplan erstellen, nach dem Kaspersky Anti-Virus Sie über die Bereitschaft eines Berichts benachrichtigen soll.

➤ Gehen Sie folgendermaßen vor, um einen Zeitplan für das Senden von Benachrichtigungen zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.
2. Im folgenden Fenster auf der Registerkarte **Bericht** aktivieren Sie das Kontrollkästchen ☒ **An Bericht erinnern**. Klicken Sie auf den Link mit dem festgelegten Zeitpunkt.
3. Im nächsten Fenster **Bericht: Zeitplan** legen Sie einen Zeitplan an.

EREIGNISTYP AUSWÄHLEN

Eine vollständige Liste aller wichtigen Ereignisse, die bei der Arbeit einer Schutzkomponente, beim Ausführen einer Untersuchungsaufgabe oder beim Update der Programm-Datenbanken eintreten, wird in einem Bericht aufgezeichnet. Sie können den Typ der Ereignisse auswählen, die im Bericht angezeigt werden sollen.

Es gibt folgende Ereignistypen:

- *Kritische Ereignisse.* Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit von Kaspersky Anti-Virus oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Dazu zählen beispielsweise ein Virenfund oder eine Funktionsstörung.
- *Wichtige Ereignisse.* Ereignisse, die unbedingt beachtet werden müssen, weil sie auf Situationen bei der Programmarbeit hinweisen, die Ihre Reaktion erfordern (z.B. Ereignis wurde **abgebrochen**).

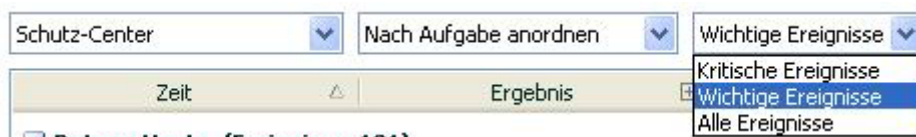


Abbildung 14. Ereignistyp wählen

Entscheiden Sie sich für den Punkt **Alle Ereignisse**, werden im Bericht alle Ereignisse angezeigt, jedoch nur dann, wenn im Abschnitt **Berichte und Speicher** im Block **Berichte** die Häkchen in den Kontrollkästchen (s. Abschnitt "Einträge über Ereignisse zum Bericht hinzufügen" auf S. 114) gesetzt sind, mit denen in den Bericht Einträge über unkritische Ereignisse sowie Ereignisse des Dateisystems und der Registrierung gemacht werden dürfen. Wenn die Kontrollkästchen nicht aktiviert sind, werden neben der Dropdown-Liste, die der Auswahl von Ereignistypen dient, ein Warnsymbol und der Link **Deaktiviert** angezeigt. Verwenden Sie diesen Link, um in das Fenster zum Anpassen von Berichten zu gehen und die entsprechenden Kontrollkästchen zu aktivieren.

➡ Gehen Sie folgendermaßen vor, um einen Ereignistyp auszuwählen, für den ein Bericht erstellt werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster in der Dropdown-Liste einen Ereignistyp aus. Wenn ein Bericht über alle Ereignisse erstellt werden soll, wählen Sie den Wert **Alle Ereignisse** aus.

DARSTELLUNG VON DATEN AUF DEM BILDSCHIRM

Die im Bericht enthaltenen Ereignisse werden in Tabellenform dargestellt. Sie können steuern, welche Informationen angezeigt werden sollen, indem Sie Beschränkungsbedingungen angeben. Führen Sie dazu links von der Überschrift der Tabellenspalte, für die eine Beschränkung festgelegt werden soll, einen Linksklick aus. Die Dropdown-Liste enthält die Beschränkungen, z.B. **Gestern** – für die Spalte **Zeit**, **E-Mail-Nachricht** – für die Spalte **Objekt** usw. Wählen Sie den erforderlichen Wert aus. Sie können die erforderliche Beschränkung auswählen. Die Datenanzeige erfolgt dann unter Berücksichtigung der festgelegten Beschränkung. Wenn alle Daten angezeigt werden sollen, wählen Sie in der Beschränkungsliste den Punkt **Alle** aus.

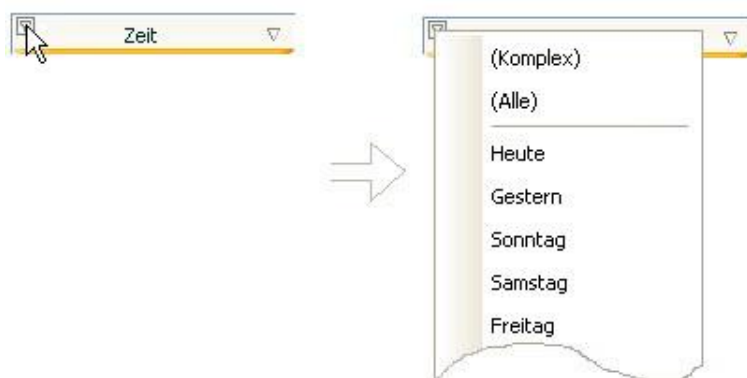


Abbildung 15. Beschränkungsbedingung festlegen

Außerdem können Sie die komplexen Suchparameter in Form eines Intervalls angeben, innerhalb dessen der Zugriff auf die vorgefallenen Ereignisse erfolgen soll. Wählen Sie dazu in der Dropdown-Liste für Beschränkungen den Punkt **Komplex** aus. Im folgenden Fenster geben Sie das gewünschte Intervall (s. Abschnitt "Verwendung der komplexen Filterung" auf S. 130) ein.

Um die Arbeit mit der Registerkarte bequem und einfach zu gestalten, gibt es ein Kontextmenü, mit dessen Hilfe der schnelle Zugriff auf ein beliebiges Merkmal möglich ist, das die Anordnung und Auswahl von Ereignissen erlaubt.



Abbildung 16. Kontextmenü

➡ Gehen Sie folgendermaßen vor, um eine Beschränkungsbedingung festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.

2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Führen Sie dazu im folgenden Fenster links von der Überschrift der Tabellenspalte, für die eine Beschränkung festgelegt werden soll, einen Linksklick aus. Wählen Sie in der Dropdown-Liste die erforderliche Beschränkung aus. Bei Entscheidung für den Punkt **Komplex** können Sie komplexe Filterbedingungen (s. Abschnitt "Verwendung der komplexen Filterung" auf S. [130](#)) eingeben.

➡ *Gehen Sie folgendermaßen vor, um die Spalten einer Tabelle auszublenden / einzublenden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Führen Sie im folgenden Fenster rechts von der Überschrift einer beliebigen Tabellenspalte einen Rechtsklick aus. Um bestimmte Spalten der Tabelle auszublenden, deaktivieren Sie im Kontextmenü die Kontrollkästchen der entsprechenden Bezeichnungen.

ERWEITERTE STATISTIKANZEIGE

Der untere Bereich des Berichtsfensters bietet eine Statistik über die Arbeit der ausgewählten Funktion oder Aufgabe von Kaspersky Anti-Virus. Sie können die Statistik als Grafik oder in Tabellenform darstellen lassen (abhängig von der Komponente oder Aufgabe). Für den Wechsel zur erweiterten Statistik dient die Schaltfläche  im oberen Bereich des Fensters. Die Statistik zeigt Informationen für den aktuellen Tag und den gesamten Zeitraum, während dem das Programm auf dem Computer arbeitet.

➡ *Gehen Sie folgendermaßen vor, um eine erweiterte Statistik anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Wählen Sie im folgenden Fenster die Programmkomponente aus, für die eine Statistik angezeigt werden soll, und verwenden Sie die Schaltfläche  im oberen Bereich des Fensters.

BERICHT IN DATEI SPEICHERN

Der Bericht kann in einer Datei gespeichert werden.

➡ *Gehen Sie folgendermaßen vor, um einen Bericht in einer Datei zu speichern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Erstellen Sie im folgenden Fenster den gewünschten Bericht und klicken Sie auf die Schaltfläche **Speichern**.
4. Geben Sie im folgenden Fenster den Ordner an, in dem die Berichtsdatei gespeichert werden soll, und nennen Sie einen Dateinamen.

VERWENDUNG DER KOMPLEXEN FILTERUNG

Das Fenster **Komplexer Filter** (s. Abbildung unten) dient dazu, die Bedingungen für die Datenfilterung zu definieren. In diesem Fenster können Sie die Intervalle für die Datensuche in einer beliebigen Spalte der Tabelle festlegen. Im Folgenden werden die Arbeitsprinzipien für dieses Fenster am Beispiel der Spalte **Zeit** beschrieben.

Der Datenzugriff mit Hilfe eines komplexen Filters basiert den Operationen Konjunktion (logisches UND) und Disjunktion (logisches ODER), mit deren Hilfe sich der Datenzugriff steuern lässt.

In den Feldern, die sich auf der rechten Seite des Fensters befinden, werden die Grenzen des Zugriffs, in diesem Fall die Zeit, angegeben. Zur Angabe der Zeit können Sie die Pfeiltasten auf der Tastatur verwenden. Auf der linken Seite, in der Dropdown-Liste **Bedingung**, werden die Zugriffsbedingungen für Ereignisse gewählt. "**Größer**" bedeutet beispielsweise größer als der im Feld rechts angegebene Wert.

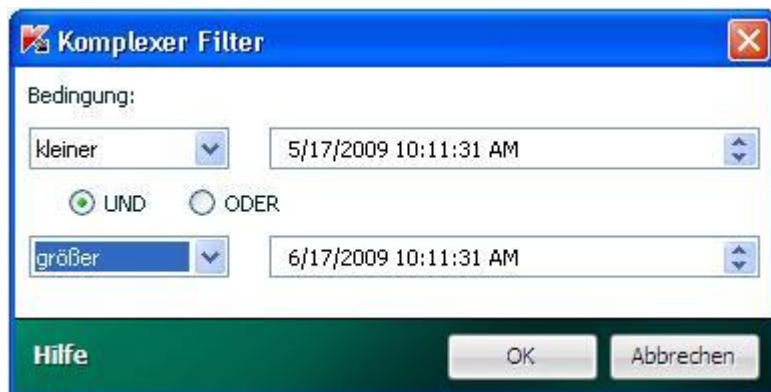


Abbildung 17. Komplexe Filterbedingungen festlegen

Wenn Sie möchten, dass er Datenzugriff beide festgelegte Bedingungen erfüllt, wählen Sie **UND** aus. Ist eine Bedingung ausreichend, dann wählen Sie **ODER** aus.

Für bestimmte Spalten gilt kein Zahlen- oder Zeitwert als Grenze des Suchintervalls, sondern ein Wort (z.B. das Untersuchungsergebnis **OK** für die Spalte **Ergebnis**). In diesem Fall wird das als Grenze angegebene Wort dem Alphabet nach mit den anderen Wortwerten für die gewählte Spalte verglichen.

➡ *Gehen Sie folgendermaßen vor, um komplexe Filterbedingungen festzulegen::*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Link **Bericht**.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Führen Sie im folgenden Fenster links von der Überschrift der Tabellenspalte, für die komplexe Filterbedingungen festgelegt werden sollen, einen Linksklick aus. Wählen Sie im Kontextmenü den Punkt **Komplex** aus. Außerdem können Sie auf den Punkt **Filter** im Kontextmenü (s. Abschnitt "Darstellung von Daten auf dem Bildschirm" auf S. 129) gehen, der mit einem Klick auf die rechte Maustaste auf die gewünschte Tabellenspalte verfügbar wird.
4. Legen Sie im folgenden Fenster **Komplexer Filter** die erforderlichen Filterbedingungen fest.

SUCHE NACH EREIGNISSEN

Dieses Fenster (siehe Abbildung unten) dient der Suche nach Ereignissen, die im System aufgetreten und von Kaspersky Anti-Virus verarbeitet wurden.

Im Folgenden werden die Prinzipien der Arbeit in diesem Fenster beschrieben:

- Das Feld **Zeile** dient der Eingabe von Schlüsselwörtern (z.B. Explorer). Klicken Sie auf die Schaltfläche **Weitersuchen**, um die Suche zu starten. Die Suche nach Daten kann eine gewisse Zeit beanspruchen. Nach Abschluss der Suche werden die Ereignisse angezeigt, die dem angegebenen Schlüsselwort entsprechen. Durch Klick auf die Schaltfläche **Alle markieren** werden alle gefundenen Daten, die dem festgelegten Schlüsselwort entsprechen, markiert.

- Das Feld **Spalte** erlaubt die Auswahl der Tabellenspalte, nach der die Suche nach dem Schlüsselwort ausgeführt wird. Eine solche Auswahl erlaubt es, die Suchdauer zu verkürzen (falls nicht der Wert **Alle** gewählt wurde).



Abbildung 18. Suche nach Ereignissen

Wenn bei der Suche die Groß- und Kleinschreibung für das Schlüsselwort berücksichtigt werden soll, aktivieren Sie das Kontrollkästchen ☒ **Groß- und Kleinschreibung**. Das Kontrollkästchen ☒ **Nur ganze Wörter** erlaubt es, die Suche nach dem Schlüsselwort auf das Vorkommen ganzer Wörter zu beschränken.

➡ *Gehen Sie folgendermaßen vor, um die Ereignissuche zu verwenden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf den Link **Bericht** im oberen Bereich des Fensters.
2. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
3. Führen Sie im folgenden Fenster rechts von der Überschrift einer beliebigen Tabellenspalte einen Rechtsklick aus. Wählen sie im Kontextmenü den Punkt **Suche** aus.
4. Legen Sie im folgenden Fenster **Suche** die Suchkriterien fest.

MELDUNGEN

Beim Auftreten bestimmter Ereignisse während der Arbeit von Kaspersky Anti-Virus werden auf dem Bildschirm spezielle Meldungen angezeigt. In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm.** Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Ein Fenster mit Meldungen dieses Typs ist rot.
- **Warnung.** Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Sie müssen entscheiden, inwieweit diese Aktion nach Ihrem Ermessen gefährlich ist. Ein Fenster mit Meldungen dieses Typs ist gelb.
- **Info.** Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Ein Fenster mit Meldungen dieses Typs ist grün.

Das Meldungsfenster besteht aus vier Elementen:

1. *Fenstertitel.* Die Überschrift der Meldung enthält eine kurze Beschreibung des Ereignisses, z.B. Anfrage auf Rechte, verdächtige Aktivität, neues Netzwerk, Alarm, Virus.
2. *Ereignisbeschreibung.* Im Block Ereignisbeschreibung werden ausführliche Informationen über den Grund für die Meldung genannt: Name des Programms, das das Ereignis hervorgerufen hat; Name der gefundenen Bedrohung; Parameter der gefundenen Netzwerkverbindung u.a.
3. *Bereich zur Aktionsauswahl.* In diesem Block können Sie eine der für dieses Ereignis möglichen Aktionen auswählen. Die zur Auswahl angebotenen Aktionen sind vom Ereignistyp abhängig, beispielsweise: **Desinfizieren**, **Löschen**, **Überspringen** – bei einem Virenfund, **Erlauben**, **Verbieten** – wenn eine Anwendung Rechte zur Ausführung potentiell gefährlicher Aktionen fordert. Die von den Kaspersky-Lab-Spezialisten empfohlene Aktion ist durch fette Schrift hervorgehoben.

Bei Auswahl der Aktion **Erlauben** oder **Verbieten** wird ein Fenster geöffnet, in dem ein *Modus für die Anwendung der Aktion* ausgewählt werden kann. Für die Aktion **Erlauben** können Sie einen der folgenden Modi auswählen:

- **Immer erlauben.** Wählen Sie diese Variante aus, um eine erkannte Programmaktivität zu erlauben und gleichzeitig die Regel für den Zugriff des Programms auf Systemressourcen entsprechend zu ändern.
- **Jetzt erlauben.** Aktivieren Sie dieses Kontrollkästchen, damit die gewählte Aktion auf alle ähnlichen Ereignisse, die während der Programmsitzung gefunden werden, angewandt wird. Als Programmsitzung gilt die Arbeitszeit ab dem Programmstart bis zum Beenden oder Neustart des Programms.
- **Vertrauenswürdig machen.** Wählen Sie diese Variante aus, um das Programm in die Gruppe **Vertrauenswürdig** zu verschieben.

Für die Aktion **Verbieten** können Sie einen der folgenden Modi auswählen:

- **Immer verbieten.** Wählen Sie diese Variante aus, um eine erkannte Programmaktivität zu verbieten und gleichzeitig die Regel für den Zugriff des Programms auf Systemressourcen entsprechend zu ändern.
 - **Jetzt verbieten.** Aktivieren Sie dieses Kontrollkästchen, damit die gewählte Aktion auf alle ähnlichen Ereignisse, die während der Programmsitzung gefunden werden, angewandt wird. Als Programmsitzung gilt die Arbeitszeit ab dem Programmstart bis zum Beenden oder Neustart des Programms.
 - **Beenden.** Wählen Sie diese Variante aus, um die Arbeit des Programms abzubrechen.
4. *Bereich zur Auswahl einer zusätzlichen Aktion.* In diesem Block kann eine zusätzliche Aktion ausgewählt werden:

- **Zu Ausnahmen hinzufügen.** Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.
- **Auf alle Objekte anwenden.** Aktivieren Sie dieses Kontrollkästchen, damit die gewählte Aktion in ähnlichen Situationen auf alle Objekte mit dem gleichen Status angewandt wird.

IN DIESEM ABSCHNITT

Verdächtiges Objekt wurde gefunden.....	134
Desinfektion des Objekts ist nicht möglich	135
Spezielle Desinfektionsprozedur ist erforderlich	135
Gefährliches Objekt wurde im Datenstrom gefunden	136
Verdächtiges Objekt wurde gefunden.....	136
Gefährliche Aktivität im System wurde erkannt	137
Versteckter Prozess wurde gefunden.....	138
Versuch zum Zugriff auf die Systemregistrierung wurde erkannt	138
Phishing-Angriff wurde erkannt	139
Verdächtiger Link wurde gefunden.....	139
Ein inkorrektes Zertifikat wurde gefunden	139

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein schädliches Objekt gefunden wird, erscheint eine spezielle Meldung auf dem Bildschirm.

Sie enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource <http://www.viruslist.com/de>, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Desinfizieren** – Es wird versucht, das schädliche Objekt zu desinfizieren. Vor der Desinfektion wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.
- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.
- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

DESINFEKTION DES OBJEKTS IST NICHT MÖGLICH

In bestimmten Fällen ist die Desinfektion eines schädlichen Objekts nicht möglich. So kann eine Datei beispielsweise so stark beschädigt sein, dass es nicht möglich ist, den schädlichen Code daraus zu löschen und sie vollständig wiederherzustellen. Außerdem ist die Desinfektionsprozedur bei einigen Arten von schädlichen Objekten wie z.B. Trojaner-Programme nicht anwendbar.

In solchen Fällen erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource <http://www.viruslist.com/de>, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.
- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gelten die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Ausschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

SPEZIELLE DESINFEKTIONSPROZEDUR IST ERFORDERLICH

Beim Fund einer Bedrohung, die gerade im System aktiv ist (beispielsweise ein schädlicher Prozess im Arbeitsspeicher oder in den Autostart-Objekten), erscheint auf dem Bildschirm eine Eingabeaufforderung zum Durchführen einer speziell dafür vorgesehenen erweiterten Desinfektionsprozedur.

Die Spezialisten von Kaspersky Lab empfehlen ausdrücklich, in solchen Fällen die erweiterte Desinfektionsprozedur durchzuführen. Klicken Sie dazu auf die Schaltfläche **OK**. Beachten Sie aber, dass zum Abschluss des Vorgangs der Computer neu gestartet wird. Deshalb sollten die aktuellen Arbeitsergebnisse gespeichert und alle Anwendungen geschlossen werden, bevor der Vorgang ausgeführt wird.

Während der Desinfektionsvorgang ausgeführt wird, sind der Start von Mailprogrammen und das Ändern der Registrierung des Betriebssystems verboten. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.

GEFÄHRLICHES OBJEKT WURDE IM DATENSTROM GEFUNDEN

Wenn Web-Anti-Virus im Datenstrom ein gefährliches Objekt findet, erscheint eine spezielle Meldung auf dem Bildschirm.

Die Meldung enthält:

- Art der Bedrohung (beispielsweise *Virusmodifikation*) und Name des gefährlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des Objekts besitzt die Form eines Links zu der Webseite <http://www.viruslist.com/de>, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Name des gefährlichen Objekts und Pfad der Web-Ressource.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Erlauben**- Download des Objekts fortsetzen.
- **Verbieten** – Download des Objekts von der Webseite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein Objekt gefunden wird, das den Code eines unbekannten Virus oder den modifizierten Code eines bekannten Virus enthält, erscheint eine spezielle Meldung auf dem Bildschirm.

Sie enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource <http://www.viruslist.com/de>, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Name und Pfad des Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Quarantäne** - Das Objekt wird in die Quarantäne verschoben. Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.
- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

GEFÄHRLICHE AKTIVITÄT IM SYSTEM WURDE ERKANNT

Wenn der Proaktive Schutz die gefährliche Aktivität einer bestimmten Anwendung im System erkennt, wird auf dem Bildschirm eine spezielle Meldung angezeigt, die folgende Informationen enthält:

- Name der Bedrohung, der ihrer Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name der Bedrohung besitzt die Form eines Links zu der Ressource <http://www.viruslist.com/de>, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Dateiname und Pfad des Prozesses, der die gefährliche Aktivität initiierte.
- Auswahl möglicher Aktionen:
 - **Quarantäne** - Prozess beenden und die ausführbare Datei des Prozesses in die Quarantäne verschieben. Wenn das Objekt in der Quarantäne gespeichert wird, wird es verschoben, nicht kopiert: Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

- **Beenden** - Prozess beenden.
- **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Anti-Virus erneut anspricht, wenn er das Programm findet.

VERSTECKTER PROZESS WURDE GEFUNDEN

Wenn der Proaktive Schutz einen versteckten Prozess im System findet, erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Name der Bedrohung, der ihrer Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name der Bedrohung besitzt die Form eines Links zu der Ressource <http://www.viruslist.com/de>, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Dateiname und Pfad des versteckten Prozesses.
- Auswahl möglicher Aktionen:
 - **Quarantäne** - Die ausführbare Prozessdatei wird in die Quarantäne verschoben. Wenn das Objekt in der Quarantäne gespeichert wird, wird es verschoben, nicht kopiert: Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

- **Beenden** - Prozess beenden.
- **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Anti-Virus erneut anspricht, wenn er das Programm findet.

VERSUCH ZUM ZUGRIFF AUF DIE SYSTEMREGISTRIERUNG WURDE ERKANNT

Wenn der Proaktive Schutz erkennt, dass versucht wird, auf Schlüssel der Systemregistrierung zuzugreifen, erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Registrierungsschlüssel, auf den der Zugriffsversuch erfolgte.
- Vollständiger Dateiname und Pfad des Prozesses, der versuchte auf Registrierungsschlüssel zuzugreifen.
- Auswahl möglicher Aktionen:
 - **Erlauben** - Das Ausführen der gefährlichen Aktion einmal erlauben.
 - **Verbieten** - Das Ausführen der gefährlichen Aktion einmal verbieten.

Damit die von Ihnen ausgewählte Aktion jedes Mal automatisch ausgeführt wird, wenn diese Aktivität auf Ihrem Computer initiiert wird, aktivieren Sie das Kontrollkästchen ☒ **Regel erstellen.**

Wenn Sie überzeugt sind, dass jede Aktivität der Anwendung, die den Zugriff auf die Systemregistrierungsschlüssel initiierte, ungefährlich ist, fügen Sie diese Anwendung der Liste der vertrauenswürdigen Anwendungen hinzu.

PHISHING-ANGRIFF WURDE ERKANNT

Wenn Kaspersky Anti-Virus einen Versuch zum Öffnen einer Phishing-Seite entdeckt, erscheint auf dem Bildschirm eine spezielle Meldung.

Die Meldung enthält folgende Informationen:

- Name der Bedrohung – *Phishing-Angriff*. Der Name besitzt die Form eines Links zur Viren-Enzyklopädie von Kaspersky Lab, wo die Bedrohung ausführlich beschrieben wird.
- Web-Adresse der Phishing-Seite im Internet.
- Auswahl möglicher Aktionen:
 - **Erlauben** – Download der Phishing-Seite fortsetzen.
 - **Verbieten** – Download der Phishing-Seite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden.** Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGER LINK WURDE GEFUNDEN

Wenn Kaspersky Anti-Virus erkennt, dass versucht wird, eine Webseite zu öffnen, deren Adresse auf der Liste der verdächtigen Webadressen steht, erscheint auf dem Bildschirm eine Meldung.

Die Meldung enthält folgende Informationen:

- Webadresse der Seite im Internet.
- Auswahl möglicher Aktionen:
 - **Erlauben** – Download der Webseite fortsetzen.
 - **Verbieten** – Download der Webseite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☒ **In allen ähnlichen Fällen anwenden.** Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

EIN INKORREKTES ZERTIFIKAT WURDE GEFUNDEN

Die Zuverlässigkeit einer SSL-Verbindung wird mit Hilfe des installierten Zertifikats geprüft. Wenn beim Verbindungsversuch mit einem Server ein inkorrektes Zertifikat verwendet wird (z.B. wenn es von einem Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine entsprechende Meldung.

Die Meldung informiert über mögliche Fehlerursachen, Remoteport und Remoteadresse. Sie werden aufgefordert zu entscheiden, ob unter Verwendung des inkorrekten Zertifikats eine Verbindung hergestellt werden soll:

- **Zertifikat akzeptieren** – Verbindung mit der Webseite fortsetzen.
- **Zertifikat ablehnen** – Verbindung mit der Webseite trennen.
- **Zertifikat anzeigen** – Informationen über das Zertifikat anzeigen.

EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS AUF KORREKTHEIT PRÜFEN

Nach der Installation und Konfiguration von Kaspersky Anti-Virus können Sie mit Hilfe eines "Testvirus" und dessen Modifikationen prüfen, ob die Einstellungen korrekt sind. Die Prüfung muss für jede Schutzkomponente und für jedes Protokoll einzeln ausgeführt werden.

IN DIESEM ABSCHNITT

EICAR-"Testvirus" und seine Modifikationen.....	141
Testen des Schutzes für HTTP-Datenverkehr.....	143
Schutz für den SMTP-Datenverkehr testen.....	143
Überprüfung der Einstellungen von Datei-Anti-Virus.....	143
Überprüfung der Einstellungen für eine Aufgabe zur Virensuche.....	144

EICAR-"TESTVIRUS" UND SEINE MODIFIKATIONEN

Dieser "Testvirus" wurde vom Institut  (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus identifiziert.

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden:
http://www.eicar.org/anti_virus_test_file.htm.

Bevor der "Testvirus" heruntergeladen wird, muss der Antiviren-Schutz deaktiviert werden, weil die Datei *anti_virus_test_file.htm* andernfalls als infiziertes, mit dem HTTP-Protokoll übertragenes Objekt identifiziert und entsprechend behandelt wird. Vergessen Sie nicht, den Antiviren-Schutz sofort nach dem Download des "Testvirus" wieder zu aktivieren.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei wird vom Programm als infiziertes Objekt identifiziert, das einen Virus enthält, **der nicht desinfiziert werden kann**, und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Funktion des Programms zu prüfen, können Sie auch Modifikationen des standardmäßigen "Testvirus" verwenden. Dazu wird der Inhalt des standardmäßigen "Testvirus" durch das Hinzufügen eines bestimmten Präfixes geändert (siehe Tabelle unten). **Zum Erstellen von Modifikationen des "Testvirus" eignet sich ein beliebiger Text-Editor oder Hypertext-Editor wie beispielsweise Microsoft Editor, UltraEdit32, usw.**

Die Prüfung der korrekten Funktion des Antiviren-Programms mit Hilfe eines modifizierten EICAR-"Testvirus" ist nur dann möglich, wenn die installierten Antiviren-Datenbanken nicht vor dem 24.10.2003 erschienen sind (kumulatives Update - Oktober 2003).

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. Die zweite Spalte zeigt die möglichen Werte für den Status, der einem Objekt aufgrund der

Untersuchungsergebnisse von Anti-Virus zugewiesen werden kann. Die dritte Spalte bietet Informationen darüber, wie Objekte mit dem betreffenden Status vom Programm bearbeitet werden. Beachten Sie, dass die Aktionen für Objekte durch die Werte der Programmparameter bestimmt werden.

Nachdem dem "Testvirus" ein Präfix hinzugefügt wurde, speichern Sie die Datei z.B. unter dem Namen *eicar_dele.com*. Verwenden Sie die in der Tabelle angegebenen Namen für die modifizierten "Viren".

Tabelle 1. Modifikationen des "Testvirus"

Präfix	Status des Objekts	Informationen zur Verarbeitung des Objekts
Kein Präfix, standardmäßiger "Testvirus".	Infiziert. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR–	Beschädigt.	Das Programm hat Zugriff auf das Objekt erhalten, kann es aber aufgrund einer Beschädigung nicht untersuchen (z.B. beschädigte Struktur des Objekts, ungültiges Dateiformat). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
WARN–	Verdächtig. Das Objekt enthält einen unbekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Objekt wurde bei der heuristischen Analyse als verdächtig erkannt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
SUSP–	Verdächtig. Das Objekt enthält den modifizierten Code eines bekannten Virus. Die Desinfektion ist nicht möglich.	Das Programm hat erkannt, dass der Objektcode teilweise mit dem Code eines bekannten Virus übereinstimmt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
ERRO–	Untersuchungsfehler.	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Die Anwendung erhielt keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
CURE–	Infiziert. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist möglich.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Das Programm führt die Desinfektion des Objekts aus, wobei der Text des Viruskörpers in CURE geändert wird. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
DELE–	Infiziert. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

TESTEN DES SCHUTZES FÜR HTTP-DATENVERKEHR

- Gehen Sie folgendermaßen vor, um die den Virenschutz für den mit HTTP-Protokoll übertragenen Datenverkehr zu prüfen:

Versuchen Sie, den "Testvirus" von der offiziellen Internetseite des **EICAR**-Instituts herunterzuladen:
http://www.eicar.org/anti_virus_test_file.htm.

Beim Versuch, den "Testvirus" herunterzuladen, erkennt Kaspersky Anti-Virus das Objekt, identifiziert es als infiziert und irreparabel, und führt die Aktion aus, die in den Einstellungen für die Untersuchung des HTTP-Datenverkehrs dafür festgelegt wurde. Wenn versucht wird, den "Testvirus" herunterzuladen, wird in der Grundeinstellung die Verbindung mit der Ressource getrennt und im Browserfenster erscheint eine Meldung darüber, dass dieses Objekt von dem Virus EICAR-Test-File infiziert ist.

SCHUTZ FÜR DEN SMTP-DATENVERKEHR TESTEN

Um den Virenschutz für den mit SMTP-Protokoll übertragenen Datenverkehr zu prüfen, können Sie ein Mailprogramm verwenden, das die Daten mit diesem Protokoll überträgt.

Es wird empfohlen, die Arbeit von Anti-Virus für ausgehende E-Mail sowohl im Briefkörper als auch in Anlagen zu testen. Um den Virenschutz im Körper einer E-Mail zu prüfen, fügen Sie den Text des standardmäßigen oder modifizierten "Testvirus" in den Briefkörper ein.

- Gehen Sie dazu folgendermaßen vor:

1. Erstellen Sie mit Hilfe des auf Ihrem Computer installierten Mailprogramms eine E-Mail im Format **Gewöhnlicher Text**.

Eine Nachricht, die den "Testvirus" enthält und das Format RTF oder HTML besitzt, wird nicht untersucht!

2. Fügen Sie den Text des standardmäßigen oder modifizierten "Testvirus" am Anfang der Nachricht ein oder hängen Sie eine Datei, die den "Testvirus" enthält, an die Nachricht an.
3. Schicken Sie die E-Mail an die Adresse des Administrators.

Das Programm erkennt das Objekt, identifiziert es als infiziert und blockiert das Senden der E-Mail.

ÜBERPRÜFUNG DER EINSTELLUNGEN VON DATEI-ANTI-VIRUS

- Gehen Sie folgendermaßen vor, um zu prüfen, ob Datei-Anti-Virus korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.
3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und führt die in den Einstellungen festgelegte Aktion aus. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über die Arbeitsergebnisse von Datei-Anti-Virus sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR EINE AUFGABE ZUR VIRENSUCHE

➡ Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Aufgabe zur Virensuche korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erstellen Sie eine neue Untersuchungsaufgabe und wählen Sie als Untersuchungsobjekt den Ordner, der die "Testviren" enthält.
3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.
4. Starten Sie die Ausführung der Untersuchungsaufgabe.

Wenn bei der Untersuchung verdächtige oder infizierte Objekte gefunden werden, werden die in den Einstellungen der Aufgabe festgelegten Aktionen ausgeführt. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über das Ausführungsergebnis der Untersuchungsaufgabe sind im Bericht über die Arbeit der Komponente enthalten.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Anti-Virus mit Hilfe der Befehlszeile steuern. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Programmkomponenten starten und beenden.
- Ausführung von Untersuchungsaufgaben starten und beenden.
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben und ihrer Statistik.
- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Module des Programms.
- Aufruf der Hilfe über die Syntax der Befehlszeile.
- Aufruf der Hilfe über die Syntax eines Befehls.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf das Programm über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Es sind folgende Befehle vorgesehen:

START	Komponente oder Aufgabe starten
STOP	Beenden der Arbeit einer Komponente oder Aufgabe (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das auf dem Interface von Kaspersky Anti-Virus festgelegt wurde)
STATUS	Bildschirmanzeige des aktuellen Status einer Komponente oder Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit einer Komponente oder Aufgabe
HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Programm-Update starten
ROLLBACK	Rückgängigmachen des zuletzt durchgeführten Updates von Kaspersky Anti-Virus (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt wurde)
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)

IMPORT	Importieren von Schutzeinstellungen für Kaspersky Anti-Virus (die Ausführung des Befehls ist nur möglich, wenn über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXPORT	Schutzparameter des Programms exportieren

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente des Programms spezifisch sind.

IN DIESEM ABSCHNITT

Steuerung von Komponenten und Aufgaben des Programms	146
Virensuche	148
Programm-Update	151
Rollback zum vorherigen Update	151
Schutzparameter exportieren	152
Schutzparameter importieren	152
Programm starten	153
Programm beenden	153
Protokolldatei anlegen	153
Hilfe anzeigen	154
Rückgabecodes der Befehlszeile	154

STEUERUNG VON KOMPONENTEN UND AUFGABEN DES PROGRAMMS

Befehlssyntax:

```
avp.com <Befehl> <Profil|Aufgabenname> [/R[A]:<Berichtsdatei>]
```

```
avp.com STOP|PAUSE <Profil|Aufgabenname> /password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

<Befehl>	Die Steuerung der Komponenten und Aufgaben von Kaspersky Anti-Virus wird mit Hilfe der folgenden Befehle ausgeführt: START – Start einer Schutzkomponente oder einer Aufgabe. STOP – Beenden einer Schutzkomponente oder einer Aufgabe. STATUS – Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen. STATISTICS – Die Statistik über die Arbeit einer Schutzkomponente oder einer Aufgabe auf dem Bildschirm anzeigen. Beachten Sie, dass der Befehl STOP nur ausgeführt wird, wenn das Kennwort eingegeben wird.
-----------------------	---

<Profil Aufgabenname>	Als Wert für den Parameter <Profil> eine beliebige Schutzkomponente von Kaspersky Anti-Virus, Module, die zu den Komponenten gehören, erstellte Untersuchungs- oder Updateaufgaben (die vom Programm standardmäßig verwendeten Werte werden in folgender Tabelle genannt). Als Wert für den Parameter <Aufgabenname> kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Updateaufgabe angegeben werden.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.
/R[A]:<Berichtsdatei>	/R:<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. /RA:<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Für den Parameter <Profil> wird einer der folgenden Werte angegeben:

RTP	Alle Schutzkomponenten. Der Befehl avp.com START RTP startet alle Schutzkomponenten, wenn der Schutz vollständig deaktiviert war. Wenn eine Komponente mit dem Befehl STOP aus der Befehlszeile beendet wurde, wird sie durch den Befehl avp.com START RTP nicht gestartet. Um die Komponente zu starten, ist der Befehl avp.com START <Profil> erforderlich, wobei als <Profil> der Wert der betreffenden Schutzkomponente verwendet wird, beispielsweise avp.com START FM.
pdm	Proaktiver Schutz
FM	Datei-Anti-Virus
EM	Mail-Anti-Virus
WM	Web-Anti-Virus Werte für die Subkomponenten von Web-Anti-Virus: httpscan (HTTP) – Untersuchung des http-Datenstroms sc – Skript-Untersuchung
IM	IM-Anti-Virus
Updater	Update
Rollback	Rollback zum vorherigen Update
Scan_My_Computer	Untersuchung des Computers
Scan_Objects	Untersuchung von Objekten

Scan_Quarantine	Quarantäne untersuchen
Scan_Rootkits	Nach Rootkits (rootkit) suchen
Scan_Startup (STARTUP)	Autostart-Objekte untersuchen
Scan_Vulnerabilities (SECURITY)	Suche nach Schwachstellen

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:

```
avp.com START FM
```

- Um die Arbeit der Kindersicherung fortzusetzen, geben Sie in der Befehlszeile ein:

```
avp.com RESUME ParCtl
```

- Um die Aufgabe zur Untersuchung des Computers zu beenden, geben Sie in der Befehlszeile ein:

```
avp.com STOP Scan_My_Computer /password=<Kennwort>
```

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Verarbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Konfigurationsdatei>] [<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die im Programm erstellten Aufgaben verwenden, die aus der Befehlszeile gestartet werden können. Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky Anti-Virus festgelegt wurden.

Beschreibung der Parameter:

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen.

Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.

<files>	Liste mit den Pfaden der Dateien und / oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.

/STARTUP	Autostart-Objekte.
/MAIL	Posteingänge.
/REMDRIVES	Alle Wechseldatenträger.
/FIXDRIVES	Alle lokalen Laufwerke.
/NETDRIVES	Alle Netzlaufwerke.
/QUARANTINE	Objekte in Quarantäne.
/ALL	Vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Der Pfad wird ohne Anführungszeichen angegeben, selbst wenn er ein Leerzeichen enthält.
<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert /i8 entspricht. Wenn Sie im automatischen Modus arbeiten, wendet Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Die Aktion ausgeführt, die dem <Aktion> entspricht, wird ignoriert.	
/i0	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
/i1	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
/i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
/i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	Nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	Nur infizierbare Dateien nach Inhalt untersuchen.
/fa	Alle Dateien untersuchen.
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen.	

Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen.
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.
-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter <seconds> angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter <size> angegeben wird.
<Konfigurationsdatei> – bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für die Antiviren-Untersuchung enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.	
/C:<Dateiname>	Die Werte der Parameter, die in der Datei <Dateiname> angegeben sind, verwenden.
<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.	
/R:<Berichtsdatei>	Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on off>	Verwendung der Technologie iChecker aktivieren / deaktivieren.
/iSwift=<on off>	Verwendung der Technologie iSwift aktivieren / deaktivieren.

Beispiele:

- *Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mailboxen sowie der Ordner Eigen e Dateien, Programme und der Datei test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Anhalten der Untersuchung von ausgewählten Objekten, Startender vollständigen Untersuchung des Computers, bei Abschluss der Untersuchung soll die Virensuche in den ausgewählten Objekten fortgesetzt werden:*

```
avp.com PAUSE Scan_Objects /password=<Kennwort>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist.2scan.txt. Für die Arbeit soll die Konfigurationsdatei scan_setting.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Datenbanken von Kaspersky Anti-Virus besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/R[A]:<Berichtsdatei>] [/C:<Dateiname>]  
[/APP=<on|off>]
```

Beschreibung der Parameter:

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	/R:<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. /RA:<Berichtsdatei> – alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
/C:<Dateiname>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit von Kaspersky Anti-Virus beim Update enthält. Die Konfigurationsdatei ist eine Textdatei, die eine Auswahl von Befehlszeilenparametern für das Update des Programms enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.
/APP=<on off>	Update der Programm-Module aktivieren / deaktivieren.

Beispiele:

➡ *Update der Programm-Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➡ *Update der Programm-Module von Kaspersky Anti-Virus, die Parameter der Konfigurationsdatei updateapp.ini verwenden::ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
ROLLBACK [/R[A]:<Berichtsdatei>] [/password=<Kennwort>]
```

Beschreibung der Parameter:

/R[A]:<Berichtsdatei>	/R:<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. /RA:<Berichtsdatei> – alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
avp.com EXPORT <Profil> <Dateiname>
```

Beschreibung der Parameter:

<Profil>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters <Profil> kann ein beliebiger Wert dienen, der im Hilfeabschnitt "Steuerung von Komponenten und Aufgaben des Programms" genannt wird.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Anti-Virus exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (<i>dat</i>) gespeichert und kann künftig verwendet werden, um die Einstellungen des Programms auf andere Computer zu übertragen. Außerdem können Sie die Konfigurationsdatei im Textformat speichern. Geben Sie dazu im Dateinamen die Endung <i>txt</i> an. Beachten Sie, dass der Import von Schutzparametern aus einer Textdatei nicht unterstützt wird. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter von Kaspersky Anti-Virus verwendet werden.

Beispiel:

```
avp.com EXPORT c:\settings.dat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky Anti-Virus importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde. <Kennwort>

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Ihr_Kennwort>
```

PROGRAMM STARTEN

Befehlssyntax:

```
avp.com
```

PROGRAMM BEENDEN

Befehlssyntax:

```
EXIT /password=<Kennwort>
```

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.
-------------------------	--

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

PROTOKOLLDATEI ANLEGEN

Das Anlegen einer Protokolldatei kann erforderlich sein, wenn bei der Arbeit mit Kaspersky Anti-Virus Probleme auftreten, deren genaue Analyse durch die Experten des Technischen Supports notwendig ist.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

Beschreibung der Parameter:

[on off]	Anlegen einer Protokolldatei aktivieren / deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den technischen Support wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.

Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zur Überfüllung der Festplatte kommen.

Beispiele:

➡ *Erstellen von Protokolldateien deaktivieren:*

```
avp.com TRACE file off
```

- Erstellen einer Tracing-Datei zum Senden an den technischen Support, mit einem maximalen Tracing-Niveau von 500:

```
avp.com TRACE file on 500
```

HILFE ANZEIGEN

Zur Anzeige der Hilfe über die Syntax der Befehlszeile dient folgender Befehl:

```
avp.com [ /? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
```

```
avp.com HELP <Befehl>
```

RÜCKGABECODES DER BEFEHLSZEILE

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben. Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

ALLGEMEINE RÜCKGABECODES	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei Ausgabenausführung
4	Aufgabenausführung wurde abgebrochen
RÜCKGABECODES FÜR AUFGABEN ZUR VIRENSUCHE	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

PROBLEME BEHEBEN

Wenn bei der Verwendung von Kaspersky Anti-Virus Probleme aufgetreten sind, prüfen Sie bitte zuerst, ob das Hilfesystem oder die Wissensdatenbank von Kaspersky Lab eine Lösung für Ihr Problem bieten (<http://support.kaspersky.com/de>). Die *Wissensdatenbank* ist ein Abschnitt der Webseite des technischen Support-Services und enthält Tipps über die Arbeit mit Kaspersky-Lab-Produkten und Antworten auf häufige Fragen. Versuchen Sie, auf dieser Ressource eine Antwort auf Ihre Frage oder eine Lösung für Ihr Problem zu finden.

➡ *Gehen Sie folgendermaßen vor, um die Wissensdatenbank zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Fensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Wissensdatenbank**.

Eine weitere Quelle, die Informationen über die Arbeit mit der Anwendung bietet, ist das Benutzerforum für Kaspersky-Lab-Produkte. Diese Quelle ist ebenfalls ein Abschnitt der Webseite des technischen Support-Services und enthält Fragen, Kommentare und Vorschläge von Programmbenutzern. Sie können die wichtigsten Themen des Forums kennen lernen, eigene Beiträge über das Programm schreiben oder Antworten auf Ihre Frage suchen.

➡ *Gehen Sie folgendermaßen vor, um die Webseite des Benutzerforums zu öffnen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Fensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Benutzerforum**.

Wenn Sie im Hilfesystem, in der Wissensdatenbank oder im Benutzerforum keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den technischen Support von Kaspersky Lab zu wenden.

IN DIESEM ABSCHNITT

Bericht über den Systemzustand erstellen	155
Protokolldatei erstellen	156
Dateien mit Daten senden	156
AVZ-Skript ausführen	157

BERICHT ÜBER DEN SYSTEMZUSTAND ERSTELLEN

Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung eines Problems unterstützen können, kann es erforderlich sein, einen Bericht über den Zustand des Systems zu erstellen. Dieser Bericht enthält ausführliche Informationen über gestartete Prozesse, geladene Module und Treiber, Erweiterungsmodule für Microsoft Internet Explorer und Microsoft Windows Explorer, offene Ports, gefundene verdächtige Objekte u.a.

Beim Erstellen des Berichts über den Systemzustand werden keine persönlichen Benutzerdaten gesammelt.

➡ *Gehen Sie folgendermaßen vor, um einen Bericht über den Systemzustand zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Im folgenden Fenster **Informationen für den Support** klicken Sie auf die Schaltfläche **Bericht über den Systemstatus erstellen**.

Der Bericht über den Systemzustand wird in den Formaten *html* und *xml* erstellt und im Archiv *sysinfo.zip* gespeichert. Nachdem das Sammeln von Daten über das System abgeschlossen wurde, können Sie einen Bericht ansehen.

➡ *Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Im folgenden Fenster **Informationen für den Support** klicken Sie auf die Schaltfläche **Anzeigen**.
5. Öffnen Sie das Archiv *sysinfo.zip*, das die Protokolldateien enthält.

PROTOKOLLDATEI ERSTELLEN

Nach der Installation von Kaspersky Anti-Virus können bei der Arbeit des Betriebssystems oder bestimmter Programme Störungen auftreten. Dies deutet höchstwahrscheinlich auf einen Konflikt von Kaspersky Anti-Virus mit einem Programm, das auf Ihrem Computer installiert ist, oder mit auf Ihrem Computer vorhandenen Treibern hin. Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung Ihres Problems unterstützen können, kann es sein, dass der Support Sie auffordert, eine Protokolldatei zu erstellen.

➡ *Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Verwenden Sie im folgenden Fenster **Informationen für den Support** die Dropdown-Liste im Block **Protokollierung**, um ein Protokollierungsniveau auszuwählen. Das Tracing-Niveau wird von dem Support-Spezialisten angegeben. Sollte diese Angabe des Supports fehlen, dann empfohlen, das Tracing-Niveau **500** einzustellen.
5. Klicken Sie auf die Schaltfläche **Aktivieren**, um den Protokollierungsvorgang zu starten.
6. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.
7. Klicken Sie auf die Schaltfläche **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Sie können mit dem Hochladen der Protokollierungsergebnisse (s. Abschnitt "Datendateien versenden" auf S. [156](#)) auf den Server von Kaspersky Lab beginnen.

DATEIEN MIT DATEN SENDEN

Nachdem die Protokolldateien und der Bericht über den Systemzustand erstellt wurden, müssen diese an den technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien mit den Daten auf den Server des technischen Supports hochzuladen, benötigen Sie eine Anfragenummer. Diese Nummer erhalten Sie in Ihrem Kaspersky Account auf der Seite des technischen Supports, wenn eine aktive Anfrage vorliegt.

➤ Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des technischen Supports hochzuladen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Im folgenden Fenster **Informationen für den Support** im Block **Aktionen** klicken Sie auf die Schaltfläche **Informationen für den Support auf den Server hochladen**.
5. Aktivieren Sie im folgenden Fenster die Kontrollkästchen neben den Dateien, die Sie an den technischen Support schicken möchten, und klicken Sie auf die Schaltfläche **Senden**.
6. Im folgenden Fenster **Anfragenummer angeben** geben Sie die Nummer an, die für Ihre Anfrage vergeben wurde, als Sie das elektronische Formular auf der Seite des technischen Supports ausgefüllt haben.

Die ausgewählten Dateien werden komprimiert und an den Server des technischen Supports gesendet.

Falls es nicht möglich ist, Kontakt mit dem technischen Support aufzunehmen, können Sie die Dateien mit Daten auf Ihrem Computer speichern.

➤ Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Im folgenden Fenster **Informationen für den Support** im Block **Aktionen** klicken Sie auf die Schaltfläche **Informationen für den Support auf den Server hochladen**.
5. Aktivieren Sie im folgenden Fenster die Kontrollkästchen neben den Dateien, die Sie an den technischen Support schicken möchten, und klicken Sie auf die Schaltfläche **Senden**.
6. Im folgenden Fenster **Anfragenummer angeben** klicken Sie auf die Schaltfläche **Abbrechen** und im folgenden Fenster bestätigen Sie das Speichern der Dateien auf dem Datenträger.
7. Geben Sie im folgenden Fenster einen Namen für das Archiv an.

Sie können daraufhin die gespeicherten Dateien an den technischen Support schicken. _

AVZ-SKRIPT AUSFÜHREN

Die Spezialisten von Kaspersky Lab analysieren Ihr Problem auf der Grundlage von Protokolldateien und eines Berichts über den Systemzustand. Das Ergebnis der Analyse besteht aus einer Reihe von Aktionen, die dazu dienen, die gefundenen Probleme zu beheben. Oft handelt es sich dabei um sehr viele Aktionen.

Um die Problembehebung zu vereinfachen, werden AVZ-Skripts verwendet. Ein AVZ-Skript ist eine Kombination von Befehlen, die es erlauben, Registrierungsschlüssel zu ändern, Dateien in die Quarantäne zu verschieben, eine Klassensuche mit der Möglichkeit der Isolierung von damit verbundenen Dateien vorzunehmen, Hooks der Typen UserMode und KernelMode zu blockieren, u.a.

Zum Starten der Skripts bietet das Programm einen *Assistenten zum Ausführen von AVZ-Skripts*. Der Assistent besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Es wird davor gewarnt, den Text eines Skripts, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Sollten bei der Skript-Ausführung Probleme auftreten, dann wenden Sie sich an den technischen Support.

➡ *Gehen Sie folgendermaßen vor, den Assistenten zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Im folgenden Fenster **Support** klicken Sie auf den Link **Protokollierung** im unteren Bereich des Fensters.
4. Im folgenden Fenster **Informationen für den Support** klicken Sie auf die Schaltfläche **AVZ-Skript ausführen**.

Wenn das Skript erfolgreich ausgeführt wurde, wird die der Assistent abgeschlossen. Falls bei der Skript-Ausführung Störungen auftreten, zeigt der Assistent eine entsprechende Meldung an.

ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Die vorliegende Erklärung beschreibt das Vorgehen zum Sammeln und zur Verwendung von Informationen, die in unten folgenden Liste genannt werden.

Die vorliegende Erklärung beschreibt das Vorgehen zum Sammeln und zur Verwendung von Informationen, die durch das Kaspersky Security Network gesammelt werden.

Um neue Bedrohungen für die Informationssicherheit und deren Ausgangspunkte zu identifizieren, um die Sicherheit für die mit Hilfe von Computern verarbeiteten Informationen der Nutzer zu erhöhen und um die Funktionen der von Kaspersky Lab entwickelten Produkte zu optimieren, kann der Nutzer Daten zur Verfügung stellen, die im Folgenden aufgezählt sind. Das Sammeln von solchen Daten erfolgt erst, nachdem der Nutzer diese Funktion im Abschnitt Feedback des Konfigurationsfensters des betreffenden Produkts aktiviert hat.

Liste der grundlegenden Daten:

- Informationen über die auf dem Computer installierte Hard- und Software, einschließlich der Version des Betriebssystems, installierte Updatepakete, Kern-Objekte, Treiber, Dienste, Erweiterungsmodule für den Microsoft Internet Explorer, Drucksystem-Plug-ins, Plug-ins für den Microsoft Windows Explorer, geladene Objekte, Elemente des Typs Active Setup, Applets, Symbolleisten, Einträge der Hosts-Datei und der Systemregistrierung, IP-Adressen, Versionen von Browsern und Mail-Clients, sowie die Versionsnummer des Kaspersky-Lab-Produkts.
- Eine individuelle ID, die einem PC vom Kaspersky Lab-Produkt zugewiesen wird.
- Informationen über den Zustand des Antiviren-Schutzes auf dem Computer, sowie Daten über alle mutmaßlich schädlichen Dateien und Aktionen (einschließlich Virusname, Datum und Uhrzeit des Funds, Namen, Größe und Pfade der infizierten Dateien, IP-Adresse des angreifenden Computers und Portnummer, auf die ein Netzwerkangriff gerichtet war, Name des mutmaßlich schädlichen Programms).
- Informationen über vom Nutzer heruntergeladene digital signierte Anwendungen (URL, Dateigröße, Name der Signatur).
- Informationen über ausführbare Anwendungen (Größe, Attribute, Erstellungsdatum, Informationen zum PE-Header, Regionalcode, Name, Ort und benutzte Kompressionsmethode).

Zusätzlich kann der Nutzer die im Folgenden aufgezählten Informationen zur Verfügung stellen:

- Dateien und / oder Teile von Dateien für eine zusätzliche Untersuchung bei Kaspersky Lab. Die genannten Dateien / oder deren Teile werden nur übertragen, wenn Sie die diesbezügliche Vereinbarung akzeptiert haben.

Es werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Die Überlassung der oben genannten Informationen ist freiwillig. Die Funktion zum Sammeln der Informationen kann jederzeit im Abschnitt Feedback des Konfigurationsfensters des entsprechenden Kaspersky-Lab-Produkts aktiviert oder deaktiviert werden.

VERWENDUNG DES CODES VON DRITTHERSTELLERN

Bei der Entwicklung von Kaspersky Anti-Virus wurde der Code von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

Bibliothek (PBSI) "Crypto-Si"	161
Bibliothek fastscript 1.9	162
Bibliothek pcre 7.4, 7.7	162
Bibliothek GNU bison parser	162
Bibliothek AGG 2.4	163
Bibliothek OpenSSL 0.9.8d	163
Bibliothek Gecko SDK 1.8	165
Bibliothek zlib 1.2	165
Bibliothek libpng 1.2.8, 1.2.29	165
Bibliothek libnkfm 2.0.5	165
Bibliothek expat 1.2, 2.0.1	165
Bibliothek Info-ZIP 5.51	166
Bibliothek Windows Installer XML (WiX) 2.0	166
Bibliothek passthru	169
Bibliothek filter	169
Bibliothek netcfg	169
Bibliothek pcre 3.0	169
Bibliothek RFC1321-based (RSA-free) MD5 library	169
Bibliothek Windows Template Library (WTL 7.5)	170
Bibliothek libjpeg 6b	172
Bibliothek libungif 3.0	174
Bibliothek libxdr	174
Bibliothek tiniconv - 1.0.0	174
Bibliothek bzip2/libbzip2 1.0.5	179
Bibliothek libspf2-1.2.9	180
Bibliothek Protocol Buffer	180

BIBLIOTHEK (PBSI) "CRYPTO-SI"

Für die Erstellung und Überprüfung elektronischer digitaler Signaturen wird die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Crypto-Si" verwendet, die von CryptoEx Ltd. (<http://www.cryptoex.ru>) entwickelt wurde.

BIBLIOTHEK FASTSCRIPT 1.9

Bei der Entwicklung des Programms wurde die Bibliothek FastScript copyright © Fast Reports Inc. verwendet. All rights reserved.

BIBLIOTHEK PCRE 7.4, 7.7

Bei der Entwicklung des Programms wurde die Bibliothek pcre 7.4, 7.7 nach den Nutzungsbedingungen der Lizenz BSD verwendet. Copyright © 1997-2008 University of Cambridge.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEK GNU BISON PARSER

Bei der Entwicklung des Programms wurde die Bibliothek bison parser skeleton 2.3 copyright © GNU Project <http://ftp.gnu.org/gnu/bison/> im Rahmen einer Sondergenehmigung verwendet.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BIBLIOTHEK AGG 2.4

Bei der Entwicklung des Programms wurde die Bibliothek AGG (Anti-Grain Geometry) 2.4 verwendet. Copyright © 2002-2005 Maxim Shemanarev. All rights reserved, mit modifizierter BSD-Lizenz.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEK OpenSSL 0.9.8d

Bei der Entwicklung des Programms wurde die Bibliothek OpenSSL 0.9.8d verwendet. Copyright © 1998-2007 The OpenSSL Project. All rights reserved, mit der Lizenz von OpenSSL License und der Original SSLeay License (<http://www.openssl.org/>).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written byEric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

BIBLIOTHEK GECKO SDK 1.8

Bei der Entwicklung des Programms wurde die Bibliothek Gecko SDK 1.8 verwendet. Copyright © Mozilla Foundation. All rights reserved, unter der Lizenz MPL 1.1 (<http://www.mozilla.org/MPL/MPL-1.1.html>). Webseite und Link zu der Distribution: http://developer.mozilla.org/en/docs/Gecko_SDK.

BIBLIOTHEK ZLIB 1.2

Bei der Entwicklung des Programms wurde die Bibliothek zlib 1.2 verwendet. Copyright © 1995-2005 Jean-loup Gailly and Mark Adler. Alle Rechte vorbehalten, nach den Nutzungsbedingungen der Lizenz zlib/libpng.

BIBLIOTHEK LIBPNG 1.2.08, 1.2.29

Bei der Entwicklung des Programms wurde die Bibliothek libpng 01.02.08, 01.02.29 verwendet. Copyright © 2004, 2006-2008 Glenn Randers-Pehrson. Alle Rechte vorbehalten, nach den Nutzungsbedingungen der Lizenz zlib/libpng.

BIBLIOTHEK LIBNKF 2.0.5

Bei der Entwicklung des Programms wurde die Bibliothek libnkf 2.0.5 verwendet. Copyright (c) KUBO Takehiro. All rights reserved.

BIBLIOTHEK EXPAT 1.2, 2.0.1

Bei der Entwicklung des Programms wurde die Bibliothek Expat 1.2, 2.0.1 verwendet. Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. Alle Rechte vorbehalten, Verwendung nach folgenden Nutzungsbedingungen:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEK INFO-ZIP 5.51

Bei der Entwicklung des Programms wurde die Bibliothek Info-ZIP 5.51 verwendet. Copyright (c) 1990-2007. Alle Rechte vorbehalten, nach den Nutzungsbedingungen der Lizenz Info-ZIP.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

BIBLIOTHEK WINDOWS INSTALLER XML (WiX) 2.0

Bei der Entwicklung des Programms wurde die Bibliothek Windows Installer XML (WiX) 2.0 verwendet. Copyright (c) Microsoft Corporation. All rights reserved, unter der Lizenz CPL 1.0 (<http://sourceforge.net/projects/wix/>).

Common Public License Version 1,0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which:

(i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such

Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEK PASSTHRU

Bei der Entwicklung des Programms wurde die Bibliothek Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation verwendet. All rights reserved.

BIBLIOTHEK FILTER

Bei der Entwicklung des Programms wurde die Bibliothek Bibliothek Ndis Sample NDIS Lightweight filter driver verwendet. Copyright (c) 2004-2005 Microsoft Corporation. All rights reserved.

BIBLIOTHEK NETCFG

Bei der Entwicklung des Programms wurde die Bibliothek Network Configuration Sample Copyright (c) 1997 Microsoft Corporation verwendet. All rights reserved.

BIBLIOTHEK PCRE 3.0

Bei der Entwicklung des Programms wurde die Bibliothek pcre 3.0 nach den Nutzungsbedingungen der Lizenz PCRE LICENCE verwendet. Copyright © 1997-1999 University of Cambridge. All rights reserved.

BIBLIOTHEK RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Bei der Entwicklung des Programms wurde die Bibliothek – RFC1321-based (RSA-free) MD5 library verwendet. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. Sie wird verbreitet unter der Lizenz zlib/libpng.

BIBLIOTHEK WINDOWS TEMPLATE LIBRARY (WTL 7.5)

Bei der Entwicklung des Programms wurde die Bibliothek Windows Template Library 7.5 verwendet. Copyright (c) 2005 Microsoft Corporation. All rights reserved, unter der Lizenz Common Public license 1.0, <http://sourceforge.net/projects/wtl/>.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

- a) it complies with the terms and conditions of this Agreement; and
- b) its license agreement:
 - i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;
 - ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;
 - iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and
 - iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

- a) it must be made available under this Agreement; and
- b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED

INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEK LIBJPEG 6B

Bei der Entwicklung des Programms wurde die Bibliothek libjpeg 6b verwendet. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. Verwendung nach folgenden Nutzungsbedingungen:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

- (1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.
- (2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".
- (3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining

code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

BIBLIOTHEK LIBUNGIF 3.0

Bei der Entwicklung des Programms wurde die Bibliothek libungif 3.0 verwendet. Copyright (c) 1997 Eric S. Raymond. Verwendung nach folgenden Nutzungsbedingungen:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEK LIBXDR

Bei der Entwicklung des Programms wurde die Bibliothek libxdr verwendet. Copyright © Sun Microsystems, Inc. Verwendung nach folgenden Nutzungsbedingungen:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

BIBLIOTHEK TINICONV - 1.0.0

Bei der Entwicklung des Programms wurde die Bibliothek tiniconv – 1.0.0 Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (<http://sourceforge.net/projects/tiniconv/>) unter der Lizenz GNU LGPL 2.1 (<http://www.gnu.org/>) verwendet.

GNU LESSER GENERAL PUBLIC LICENSE v.2,1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BIBLIOTHEK BZIP2/LIBBZIP2 1.0.5

Bei der Entwicklung des Programms wurde die Bibliothek bzip2/libbzip2 1.0.5 verwendet. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. Verwendung nach folgenden Nutzungsbedingungen:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

BIBLIOTHEK LIBSPF2-1.2.9

Bei der Entwicklung des Programms wurde die Bibliothek libspf2-1.2.9 verwendet. Copyright 2005 by Shevek and Wayne Schlitt, all rights reserved, Verwendung nach den Nutzungsbedingungen von The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEK PROTOCOL BUFFER

Bei der Entwicklung des Programms wurde die Bibliothek Protocol Buffer verwendet. Copyright 2008, Google Inc. All rights reserved, Sie wird verbreitet nach den Nutzungsbedingungen von New BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSAR

Eine Liste der Masken und Webressourcen, deren Inhalt der Benutzer vertraut. Webseiten, die einem Element dieser Liste entsprechen, werden von der Kaspersky Lab Software nicht auf das Vorhandensein schädlicher Objekte untersucht.

2

2-CHANNEL-GATEWAY

Computer mit zwei Netzwerkadaptern, die an verschiedene Netzwerke angeschlossen sind und Daten von einem Netzwerk an ein anderes Netzwerk übermitteln.

A

AKTIVE LIZENZ

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

ALTERNATIVE NTFS-DATENSTRÖME

Datenströme des NTFS-Dateisystems (alternate data streams), die für zusätzliche Attribute oder Datei-Informationen vorgesehen sind.

Jede Datei im NTFS-Dateisystem stellt eine Auswahl von Datenströmen (streams) dar. In einem Datenstrom befindet sich der Datei-Inhalt, den man sehen kann, wenn man die Datei öffnet, die übrigen (alternativen) Datenströme sind für Meta-Informationen vorgesehen und bieten zum Beispiel die Kompatibilität des NTFS-Systems mit anderen Systemen, wie mit dem alten Dateisystem von Macintosh - Hierarchical File System (HFS). Die Datenströme lassen sich erstellen, löschen, separat speichern, umbenennen und sogar als Prozess starten.

Alternative Datenströme können von Angreifern missbraucht werden, um Daten des Computers heimlich zu übertragen oder zu empfangen.

ARCHIV

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

AUFGABE

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind, Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbank-Update.

AUFGABENEINSTELLUNGEN

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

AUSNAHME

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

AUTOSTART-OBJEKTE

Auswahl von Programmen, die für den Start und die korrekte Funktion des auf Ihrem Computer installierten Betriebssystems und der vorhandenen Software erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell diese Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B**BACKUP**

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

BENACHRICHTIGUNGSVORLAGE

Vorlage, mit der bei der Untersuchung erkannte infizierte Objekte gemeldet werden. Eine Benachrichtigungsvorlage enthält mehrere Einstellungen, die die Reihenfolge der Benachrichtigung, die Verbreitungsart und den Meldungstext definieren.

BOOTVIRUS

Virus, der die Bootsektoren von Computerlaufwerken infiziert. Der Virus "zwingt" das System beim Hochfahren, nicht auf den eigentlichen Bootcode zuzugreifen, sondern auf den Viruscode, der dann die Kontrolle übernimmt.

D**DATEIMASKE**

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind * und ? (wobei * für eine beliebige Anzahl von Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR VERDÄCHTIGE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als potentiell gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen. Um die Erkennungsqualität für Bedrohungen zu steigern, empfehlen wir, regelmäßig Updates für die Datenbanken von den Kaspersky-Lab-Updateservern herunterzuladen.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbanken. Bei der Desinfektion können Daten teilweise verloren gehen.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

DOMAIN NAME SERVICE (DNS)

Verbreitetes System zur Umformung von Hostnamen (Computer oder anderes Netzwerkgerät) in eine IP-Adresse. DNS funktioniert in TCP/IP-Netzwerken. Im Einzelfall kann DNS auch umgekehrte Anfragen und Definitionen von Hostnamen nach dessen IP (PTR-Eintrag) speichern und verarbeiten. Die Auflösung von DNS-Namen erfolgt gewöhnlich durch Netzwerkprogramme und nicht durch die Benutzer.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

E

ECHTZEITSCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

EIN- UND AUSGABEPORT

Wird in Mikroprozessoren (z.B. Intel) beim Datenaustausch mit der Hardware verwendet. Der Ein- und Ausgabeport wird einem bestimmten Gerät zugeordnet und erlaubt es den Programmen, zum Datenaustausch darauf zuzugreifen.

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, das Kaspersky-Lab-Programm mit allen Funktionen zu nutzen. Die Gültigkeitsdauer der Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Gültigkeitsdauer der Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr verfügbar.

H

HARDWARE-PORT

Eingang an einem Hardware-Element des Computers, an den ein Kabel oder ein Stecker angeschlossen werden kann (LPT-Port, serieller Port, USB).

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die sich nicht mit Hilfe der Datenbanken von Anti-Virus identifizieren lassen. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Antiviren-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen der Technologie iChecker:

- Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.
- Die Technologie unterstützt eine begrenzte Anzahl von Formaten (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

INDIKATOR FÜR EINE VIRENEPIDEMIE

Vorlage, auf der eine Benachrichtigung über den drohenden Ausbruch einer Virenepidemie beruht. Der Indikator für eine Virenepidemie umfasst einige Einstellungen, die den Schwellenwert der Virenaktivität, die Verbreitungsart und den Meldungstext enthalten.

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines anderen Herstellers oder Programm von Kaspersky Lab, das nicht mit Kaspersky Anti-Virus verwaltet werden kann.

INSTALLATION MIT STARTSZENARIO

Remote-Installation von Kaspersky-Lab-Programmen, mit der der Start der Aufgabe zur Remote-Installation mit einem konkreten Benutzerkonto (mehreren Benutzerkonten) verknüpft werden kann. Beim Anmelden des Benutzers in der Domäne wird versucht, das Programm auf dem Client-Computer zu installieren, auf dem sich der Benutzer angemeldet hat. Dieses Verfahren wird für die Installation von Programmen des Herstellers auf Computern empfohlen, die mit den Betriebssystemen Microsoft Windows 98 / Me laufen.

INTERCEPTOR

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

INTERNETPROTOKOLL (IP)

Basisprotokoll für das Internet, das seit seiner Entwicklung im Jahre 1974 unverändert verwendet wird. Es führt die Grundoperationen bei der Datenübertragung von einem Computer auf einen anderen aus und dient als Basis für alle Protokolle höherer Ebenen wie TCP und UDP. Es kontrolliert die Verbindung und die Fehlerbehandlung. Technologien wie IPv4 und Maskierung ermöglichen es, umfangreiche Netzwerke hinter einer relativ geringen Anzahl von IP-Adressen

zu verbergen (oder sogar hinter einer Adresse). Dadurch wird erlaubt, die Ansprüche des ständig expandierenden Internets unter Verwendung eines relativ begrenzten IPv4-Adressraums zu befriedigen.

K

KASPERSKY-LAB-UPDATESERVER

Liste der http- und ftp-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

KONTROLLIERTES OBJEKT

Datei, die mit den Protokollen HTTP, FTP oder SMTP übertragen und von der Firewall zur Untersuchung durch das Kaspersky-Lab-Programm umgeleitet wird.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält z.B. Angaben über Absender, Empfänger und Datum.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

LISTE DER ZU UNTERSUCHENDEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, die vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte unbedingt untersucht werden sollen.

M

MAIL-DATENBANKEN

Datenbanken mit einem speziellem Format, in denen die auf Ihrem Computer gespeicherten E-Mails enthalten sind. Jede eingehende / ausgehende E-Mail wird nach dem Empfang / Senden in einer Mail-Datenbank gespeichert. Solche Datenbanken werden bei einer vollständigen Untersuchung des Computers untersucht.

Eingehende und ausgehende E-Mails werden im Augenblick des Empfangs und Sendens in Echtzeit auf Viren analysiert, wenn der Echtzeitschutz aktiviert ist.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

N

NETZWERKPORT

Parameter für die Protokolle TCP und UDP, der den Zweck von Datenpaketen im IP-Format definiert, die über ein Netzwerk auf einen Host übertragen werden. Er erlaubt unterschiedlichen auf einem Host ausgeführten Programmen, unabhängig voneinander Daten zu empfangen. Jedes Programm verarbeitet die Daten, die auf einem bestimmten Port eintreffen (man sagt auch, ein Programm "hört" einen bestimmten Port).

Gewöhnlich sind häufig verwendeten Netzwerkprotokollen standardmäßige Portnummern zugeordnet (Webserver empfangen ihre Daten standardmäßig mit dem HTTP-Protokoll auf TCP-Port 80), obwohl ein Programm prinzipiell ein beliebiges Protokoll und einen beliebigen Port verwenden kann. Mögliche Werte: von 1 bis 65535.

O

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

P

POTENTIELL INFIZIERBARES OBJEKT

Ein Objekt, das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmal eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

- **Kritisches Ereignis.**
- **Funktionsstörung.**
- **Warnung.**
- **Informative Meldung.**

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

PROGRAMM AKTIVIEREN

Der Aktivierungsvorgang für das Programm umfasst die Eingabe eines Aktivierungscodes und den anschließenden Download eines Schlüssels, mit dem das Programm prüft, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer dafür gilt.

PROGRAMM-MODULE

Dateien, die zum Lieferumfang von Kaspersky Lab gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jeder Art von Aufgaben, die das Programm realisiert (Echtzeitschutz, Virensuche, Update), entspricht ein eigenes

ausführbares Modul. Wenn die vollständige Untersuchung Ihres Computers aus dem Hauptfenster gestartet wird, initiieren Sie den Start des Moduls für diese Aufgabe.

PROGRAMMEINSTELLUNGEN

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen, zum Beispiel Parameter für die Leistungsfähigkeit des Programms, Parameter für das Berichtswesen, Backup-Parameter.

PROTOKOLL

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind z.B. HTTP (WWW), FTP und NNTP (News).

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an anderen Netzwerkservern richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.

Q

QUARANTÄNE.

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

R

RESERVELICENSE

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Eine Reserve-Lizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

S

SOCKS

Proxyserver-Protokoll, mit dem eine zweiseitige Verbindung zwischen Computern eines lokalen und externen Netzwerks realisiert werden kann.

SCHLÜSSELDATEI

Datei mit der Endung .key, die Ihr persönlicher "Schlüssel" ist und für die Arbeit des Kaspersky-Lab-Programms erforderlich ist. Eine Schlüsseldatei ist im Lieferumfang des Produkts enthalten, wenn es bei einem Händler von Kaspersky Lab erworben wurde, oder sie wird Ihnen per E-Mail zugesandt, wenn das Produkt in einem Internet-Shop gekauft wurde.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Datenbank, die Informationen über von Kaspersky Lab gesperrte Schlüsseldateien enthält, deren Besitzer gegen die Bedingungen des Lizenzvertrags verstoßen haben, und über Schlüsseldateien, die zwar ausgegeben, aber nicht verkauft oder ersetzt wurden. Die Datei mit der schwarzen Liste ist für die Arbeit von Kaspersky-Lab-Programmen erforderlich. Die Datei wird gemeinsam mit den Datenbanken aktualisiert.

SCHWELLE FÜR VIRENAKTIVITÄT

Maximal zulässige Anzahl von Ereignissen eines bestimmten Typs innerhalb eines festgelegten Zeitraums, deren Überschreitung als erhöhte Virenaktivität und als Anzeichen eines Virenangriffs gilt. Dieser Wert besitzt insbesondere bei Viren-Epidemien große Bedeutung und erlaubt es dem Administrator, rechtzeitig auf drohende Virenangriffe zu reagieren.

SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Komponente verstanden.

SICHERUNGSKOPIEREN

Bevor ein Desinfektionsversuch erfolgt oder die Datei gelöscht wird, legt die Anwendung eine Sicherungskopie an und speichert diese im Backup. Dadurch wird ermöglicht, die Datei bei Bedarf wiederherzustellen, um sie beispielsweise mit aktualisierten Datenbanken zu untersuchen.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripts werden beispielsweise gestartet, wenn Sie eine bestimmte Webseite öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripts, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

U

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (z.B. HTTP, FTP u.a.). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket, das der Softwareaktualisierung dient, aus dem Internet kopiert und auf Ihrem Computer installiert wird.

V

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

VERFÜGBARES UPDATE

Updatepaket für die Module einer Kaspersky-Lab-Anwendung, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Anwendungsarchitektur enthält.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

W**WIEDERHERSTELLUNG**

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

Z**ZERTIFIKAT DES ADMINISTRATIONSSERVERS**

Zertifikat, mit dem der Administrationsserver beim Herstellen einer Verbindung mit der Administrationskonsole und Datenaustausch mit den Client-Computern authentifiziert wird. Das Zertifikat des Administrationsservers wird bei Installation des Administrationsservers angelegt und im Unterordner Cert des Installationsverzeichnisses gespeichert.

ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN“ KLIKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESER VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN“ GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

- 1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.
- 1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.
- 1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.
- 1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff „Sie“ weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff „Organisation“ ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.
- 1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.
- 1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.
- 1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung

- 2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.
Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der

Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Lizenzen, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die Lizenzbedingungen sehen eine anderweitige Regelung vor.*

- 2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.
- 2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software gekauft haben.
- 2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.
- 2.5. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen oder Rechtspersönlichkeiten innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.
- 2.6. Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Kaufs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:
 - Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
 - Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

- 3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.
- 3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.
- 3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Kaufs bezeichnete Zeitdauer genutzt werden.
- 3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt.
- 3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.
- 3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.
- 3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.
- 3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen,

nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

- 3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

4. Technische Unterstützung

Die in Klausel 2.6 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).

Technischer Support: <http://support.kaspersky.com>

5. Sammeln von Informationen

- 5.1. Durch Zustimmung zu den Geschäftsbedingungen dieses Vertrags haben Sie eingewilligt, dem Rechtsinhaber Informationen über die ausführbaren Dateien und ihre Prüfsummen zur Verfügung zu stellen, um Ihr Sicherheits-Schutzniveau zu verbessern.
- 5.2. Um das Sicherheitsbewusstsein bezüglich neuer Bedrohungen und deren Quellen zu verbessern, bzw. um Ihr Sicherheits-Schutzniveau zu verbessern, ist der Rechtsinhaber ausdrücklich berechtigt, mit Ihrer Zustimmung, die ausdrücklich in der Kaspersky Security Network Datenerfassungserklärung bestätigt wurde, derartige Informationen zu empfangen. Sie können den Kaspersky Security Network Service während der Installation deaktivieren. Sie können ebenfalls jederzeit auf der Softwareoptionsseite den Kaspersky Security Network Service aktivieren und deaktivieren.

Sie bestätigen und erkennen weiterhin an, dass jedwede Informationen, die vom Rechtsinhaber erfasst werden, zum Zweck der Verfolgung und Veröffentlichung von Sicherheitsrisikotrends verwendet werden können, und zwar nach freiem Ermessen des Rechtsinhabers.

- 5.3. Die Software verarbeitet keine personenbezogenen Daten und kombiniert keine Verarbeitungsdaten und persönlichen Informationen.
- 5.4. Sollten Sie nicht wünschen, dass die von der Software gesammelten Informationen an den Rechtsinhaber geschickt werden, sollten Sie den Kaspersky Security Network Service nicht aktivieren und/oder deaktivieren.

6. Beschränkungen

- 6.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompileieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.
- 6.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.5 dieses Vertrags.
- 6.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.5 dieses Vertrags an Drittparteien übertragen dürfen.
- 6.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.
- 6.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.
- 6.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.
- 6.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

7. Eingeschränkte Garantie und Haftungsausschluss

- 7.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt*, dass eine solche

eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

- 7.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.
- 7.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.
- 7.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.6 dieses Vertrags erläutert, Updates herunterladen.
- 7.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.
- 7.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISSKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGEGEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

8. Haftungsausschluss und Haftungsbeschränkungen

INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGEND EINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

9. GNU und sonstige Drittpartei-Lizenzen

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

10. Geistiges Eigentum

- 10.1 Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.
- 10.2 Sie bestätigen, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüssel-Datei für die Software Eigentum des Rechtsinhabers sind und Geschäftsgeheimnisse des Rechtsinhabers konstituieren. Sie stimmen zu, den Quellcode der Software nicht zu modifizieren, abzuwandeln, zu übersetzen, zurückzuentwickeln, zu dekompileieren oder auf sonstige Weise zu versuchen, den Quellcode ausfindig zu machen.
- 10.3 Sie stimmen zu, die Software in keinsten Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

11. Geltendes Recht; Schiedsverfahren

Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von

jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

12. Zeitraum für Rechtsverfolgung.

Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

13. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

14. Kontaktinformationen.

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Dokortitel besitzen. Die führenden Virusanalysen von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahrungen, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus® und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab: <http://www.kaspersky.de>

Viren-Enzyklopädie: <http://www.viruslist.com/de/>

Antiviren-Labor: newvirus@kaspersky.com
(nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>
(für Fragen an die Virenanalytiker)

Webforum von Kaspersky Lab: <http://forum.kaspersky.com>

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Dokortitel besitzen. Die führenden Virusanalysen von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahrungen, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus® und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab: <http://www.kaspersky.de>

Viren-Enzyklopädie: <http://www.viruslist.com/de/>

Antiviren-Labor: newvirus@kaspersky.com
(nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>
(für Fragen an die Virenanalytiker)

Webforum von Kaspersky Lab: <http://forum.kaspersky.com>

SACHREGISTER

A

Algorithmus für die Arbeit	
Mail-Anti-Virus	53
Algorithmus für die Arbeit	
Datei-Anti-Virus	43
Algorithmus für die Arbeit	
Web-Anti-Virus	60
Algorithmus für die Arbeit	
IM-Anti-Virus	67

B

Backup	116
Berichte	
Ereignistyp	128
Filterung	130
in Datei speichern	130
Komponente oder Aufgabe auswählen	126
Suche nach Ereignissen	131
BERICHTE	126
Browser-Konfiguration	123

D

Datei-Anti-Virus	
Arbeit anhalten	49, 50
Algorithmus für die Arbeit	43
Heuristische Analyse	46
Reaktion auf die Bedrohung	44
Schutzbereich	45
Sicherheitsstufe	44
Standardparameter wiederherstellen	51
Untersuchung optimieren	47
Untersuchung von zusammengesetzten Dateien	47
Untersuchungsmodus	48
Untersuchungstechnologie	48
Datenbank für Phishing-Webadressen	
IM-Anti-Virus	67
Web-Anti-Virus	62

E

Echtzeitschutz des Computers deaktivieren / aktivieren	94
--	----

H

Heuristische Analyse	
Datei-Anti-Virus	46
IM-Anti-Virus	68
Mail-Anti-Virus	57
Web-Anti-Virus	64

I

IM-Anti-Virus	
Algorithmus für die Arbeit	67
Datenbank für Phishing-Webadressen	67
Heuristische Analyse	68
Schutzbereich	67

K

Kaspersky Anti-Virus beim Hochfahren des Betriebssystems starten.....	95
Kategorien der erkennbaren Bedrohungen	105
Kontextmenü	38
Kontrolle des Zugriffs auf das Programm	96

L

Leistung des Computers.....	103
-----------------------------	-----

M

Mail-Anti-Virus	
Algorithmus für die Arbeit.....	53
Anlagenfilterung	57
Heuristische Analyse	57
Reaktion auf die Bedrohung	54
Schutzbereich	55
Sicherheitsstufe	53
Standardparameter wiederherstellen	58
Untersuchung von zusammengesetzten Dateien	57
Modul zur Link-Untersuchung	
Web-Anti-Virus.....	63

N

Netzwerk	
geschützte Verbindungen	109
Notfall-CD	121

P

Proaktiver Schutz	
Kontrolle über Systembenutzerkonten	71
Regel für die Kontrolle einer gefährlichen Aktivität	70
Programmhauptfenster	39
Programmkomponenten	15
PROGRAMMOBERFLÄCHE.....	37

Q

Quarantäne und Backup.....	115
Quarantäne.	115

R

Reaktion auf die Bedrohung	
Datei-Anti-Virus.....	44
Mail-Anti-Virus	54
Virensuche.....	76
Web-Anti-Virus.....	61

S

Schutzbereich	
Datei-Anti-Virus.....	45
IM-Anti-Virus	67
Mail-Anti-Virus	55
Web-Anti-Virus.....	62
Selbstschutz für das Programm	101
Sicherheitsstufe	
Datei-Anti-Virus.....	44
Mail-Anti-Virus	53

Web-Anti-Virus.....	61
Standardparameter wiederherstellen	
Datei-Anti-Virus.....	51
Mail-Anti-Virus	58
Suche nach Schwachstellen	
Benutzerkonto.....	85
Liste der Untersuchungsobjekte	84
Zeitplan.....	85
Symbol im Infobereich der Taskleiste.....	37

U

Untersuchung	
Aktion für ein gefundenes Objekt.....	76
Aufgabe starten	74
automatischer Start einer übersprungenen Aufgabe	81
Benutzerkonto.....	81
Sicherheitsstufe	76
Suche nach Schwachstellen.....	82
Typ der zu untersuchenden Objekte	77
Untersuchung optimieren.....	78
Untersuchung von zusammengesetzten Dateien	79
Untersuchungstechnologien	79
Zeitplan.....	81
Update	
aus einem lokalen Ordner.....	91
Proxyserver verwenden	90
Regionsoptionen.....	90
Rollback zum vorherigen Update	89
Updatequelle.....	89

V

Vertrauenswürdige Zone	
Regeln für Ausnahmen	106
Vertrauenswürdige Anwendungen.....	105
Virtuelle Tastatur	120

W

Web-Anti-Virus	
Algorithmus für die Arbeit.....	60
Datenbank für Phishing-Webadressen	62
Heuristische Analyse	64
Modul zur Link-Untersuchung.....	63
Reaktion auf die Bedrohung	61
Schutzbereich	62
Sicherheitsstufe	61
Untersuchung optimieren.....	64

Z

Zeitplan	
Update	91
Virensuche.....	81